وزارة التّعليم العالي و البحث العلمي
جامعة – باتنة 1
كلــية الحــقوق و العلوم الســياسية
قــسم الــحقوق

آليات البحث و التحقيق في الجرائم المعلوماتية

أطروحة مقدّمة لنيل شهادة دكتوراه العلوم
في الحقوق تخصّص –قانون العقوبات و العلوم الجنائية

إعـــداد الطّالـــب:
ربيعـــــي حســـــين

تحـــــــت إشـــــــراف:
الأســتاذة الــدّكتورة رحــاب شــادية

أمام لجنة المناقشة المكوّنة من:

د/ فايزة ميموني	أستاذ محاضر –أ–	جامعة باتنة 1	رئيسا
أ.د/ شادية رحاب	أستاذ التعليم العالي	جامعة باتنة 1	مشرفا و مقررا
أ.د/ عبد الحليم بن مشري	أستاذ التعليم العالي	جامعة محمد خيضر بسكرة	عضوا مناقشا
أ.د/ العيد سعادنة	أستاذ التعليم العالي	جامعة عباس لغرور خنشلة	عضوا مناقشا
د/ لخضر زرارة	أستاذ محاضر –أ–	جامعة باتنة 1	عضوا مناقشا
د/عادل مستاري	أستاذ محاضر –أ–	جامعة محمد خيضر بسكرة	عضوا مناقشا

الموسم الجامعي 2015-2016

«بسم الله الرحمن الرحيم»

«وَ مَا تَوفِيقِيَ إلاَ بِالله عَلَيهِ تَوَكَلتُ وِ إِلَيهِ أُنِيبُ»

سورة هود الآية (88)

قال الأصفهاني« إني رأيت أنه لا يكتب إنسانٌ كتاباً في يومه إلا قال في غده :لو غُيرَ هذا لكان أحسن ،و لو زِيدَ هذا لكان يستحسن ،و لو قُدمَ هذا لكان أفضل ،ولو تُركَ هذا لكان أجمل، و هذا من أعظم العبر و هو خير دليل على إستيلاء النقص على جملة البشر »

شكر و إمتنان

إلى أحب الناس إلى قلبي و أقربهم إلى روحي، إلى أحب من في الوجود

أمي أبي زوجتي أبنائي إخوتي.

- إلى من فارقتني بجسدها ولم تفارقني بروحها جدتي .
- إلى كل زملائي و زميلاتي ، إلى كل الذين وقفوا إلى جانبي و سهلوا علي طريق البحث و لو بالكلمة ،الإبتسامة ، الشعور الصادق.
- إلى كل من عرفتهم خلال مشواري الدراسي و أحبوني بصدق و إخلاص إلى كل هؤلاء

لكم مني جزيل الشكر و الإمتنان و جزاكم الله عني خير الجزاء.

أضع هذا العمل المتواضع بين يدي كل محب للعلم و ساع وراءه، راجيا من المولى تعالى أن يضيفه لي في ميزان أعمالي، و أن يتقبله خالصا لوجهه الكريم.

شكر خاص

أتقدم بالشكر الجزيل في هذا المقام أولا إلى الدكتورة القديرة و الأستاذة المحترمة رحاب شادية على قبولها مهمة الإشراف على أطروحتي هذه و هي التي لم تبخل علي بنصائحها القيمة النابعة من تجربتها الطويلة في ميدان البحث العلمي ، و متابعتها المتواصلة لأطوار إنجاز هذا البحث، و صبرها الطويل علي فلكي مني أستاذتي الفاضلة أزكى عبارات الشكر و التقدير.

كما لا يفوتوني أن أتقدم بالشكر إلى كل أعضاء اللجنة المحترمة الذين و بالإضافة إلى إنشغالاتهم المتعلقة بأداء مهام تبليغ الرسالة العلمية،إلا أنهم أبوا إلا أن يشاركوا في مناقشة هذا العمل يدفعهم إلى ذلك هدف نبيل و هو تطوير مجالات المعرفة العلمية.

- قائمة بأهم الرموز:

- أولا: باللغة العربية:

- ق إ ج : قانون الإجراءات الجزائية الجزائري.
- ق ع : قانون العقوبات.
- ص: صفحة.
- ق : قانون.

- ثانيا: باللغة الفرنسية:

- P : page
- Op. Cit. : Abréviation utilisée dans les notes bibliographiques pour faire référence à un Ouvrage précédemment cité.
- Ibid. : Abréviation utilisée dans les notes bibliographiques pour faire référence à un ouvrage déjà cité dans une note précédente.

مقدمة

أولا – التعريف بالموضوع.

لقد شهدت البشرية في ظرف وجيز من الزمن ، مقارنة بما سبق من عهد التاريخ البشري تطورا فائقا نقلها نقلة نوعية من عالم إلى أخر ، فتحولت عديد مظاهر الحياة من كل ما هو تقليدي و مادي ، إلى ما هو حديث و رقمي ، و ذلك بفعل إنتشار تقنية المعلوماتية في حقبة السبعينيات من القرن الماضي ، فأصبحت الإستعمالات اليومية للحواسيب و شبكات الإتصال أمرا شائعا داخل أغلب المجتمعات المتحضرة ، و قد تغلغلت التقنية المعلوماتية في كل جوانب الحياة ، فأصبحت و بما توفره من تسهيلات و بفضل ما تشهده من تطور مستمر و دائم ، التقنية الأولى و بدون منازع التي تستعين بها المجتمعات في شتى مجالات حياتهم ، و ذلك من خلال الإعتماد عليها للتحكم في تسيير المرافق الحيوية للدول و الحكومات ، كالإدارة الإلكترونية ، و مجلات الدفاع و الأمن ، و الإقتصاد و الصحة...إلـــخ ، و هي و بالإضافة لذلك تشهد إنتشاراً واسع النطاق على المستوى الإجتماعي ، فأفراد المجتمعات أصبحوا يديرون شؤون حياتهم اليومية من خلال مجموعة التطبيقات التي توفرها تقنية المعلوماتية ، كالتواصل المباشر و تبادل المعارف و المعلومات ، و التعاقد عن بعد عن طريق شبكة الأنترنت، بل و قضاء كل ما كان مستعصياً من قبل بفعل العوائق الجغرافية و المادية ، و التي أصبحت في ظل عالم المعلوماتية مجرد أرقام و رموز إلكترونية ، و التي لا يتطلب أمر تجاوزها سوى الكبس على زر من أزرار لوحة مفاتيح الحاسوب ، و بذلك فقد غيرت هذه التقنية من نمط الحياة البشرية فإرتقت بها و جعلت منها حياة أفضل تميزها السرعة و التطور و اليسر .

غير أن كل هذا التطور و التحول في أسلوب حياة الإنسان حمل معه مظاهر سلبية ، أثرت على أمن الدول و الأفراد بالسلب ، و ذلك من خلال ظهور صور الإستعمال غير المشروع لتقنية المعلوماتية ، و هي التي أصطلح عليها قانونا وصف " الجرائم المعلوماتية" ، هذا النوع الحديث من السلوكات الإجرامية الماسة بأمن و سلامة النظم المعلوماتية و بحقوق الغير تشكل خطرا بالغا و ذلك لتعدد

أوصافها الإجرامية ، كجرائم سرقة المعلومات المخزنة أو تخريبها ، أو جرائم التحويل غير المشروع للأموال ، أو جرائم التعدي على الغير عبر الشبكات ، أو جرائم الإستغلال الجنسي للقصر و الأطفال...ألــخ من جرائم مستحدثة تتسم بطابعها المعنوي الخالص ، و تخلو من الطابع المادي المميز لأغلب الجرائم التقليدية .

إن ظهور كل هذه المفاهيم الإجرامية الحديثة ، قلب مفاهيم النظرية التقليدية للجريمة ، فقد أدخلت الجريمة المعلوماتية على هذه الأخيرة صورا جديدة للجريمة بركنها الشرعي ، و أساليب و طرق حديثة لم تكن معروفة من قبل مست الجريمة من خلال ركنها المادي ، فالجرائم المعلوماتية جرائم ناعمة ، لا تستوجب لتحقيقها وسائلاً و جهداً ماديا كبيرا ، و ذلك من خلال إعتماد الجناة على وسائل تكنولوجية و أساليب إجرامية حديثة و متطورة تسمح لهم بنيل مبتغاهم بأقل جهد و بأسرع وقت ممكن دون اللجوء إلى العنف المادي ، فمجرمو المعلوماتية يتميزون بالذكاء و المعرفة الواسعة بمجال المعلوماتية و أدق تفاصيلها ، و هو ما يسمح لهم كذلك بالتحكم في أثار و أدلة جرائمهم من خلال تدميرها و محوها و هو ما يجعل من امر أغلب الجرائم المعلوماتية خفية لا يمكن إكتشافها أو تتبع أثارها ، بالنظر إلى الطبيعة الخاصة للأدلة الناتجة عن هذا النوع من الجرائم ، و التي أصبحت تشكل التحدي الأكبر الذي يواجه النصوص الجزائية الإجرائية ، التي تنظم سير جملة الإجراءات الخاصة بعمليات البحث و التحقيق و ملاحقة المجرمين ، في إطار شرعي من أجل تقديمهم امام العدالة ، فالجريمة المعلوماتية بوصفها " ذلك السلوك الإجرامي المنصب على استعمال تقنية المعلوماتية ، بهدف التعدي على أمن سلامة النظم المعلوماتية و جملة المعلومات المتداولة عبرها ، من خلال شبكات الإتصال ، او تلك المخزنة على ذاكرة الحواسيب المتصلة بها " ، تشكل نقطة تعارض بين التكنولوجيا الحديثة و جملة النصوص القانونية الإجرائية ، فهذه الأخيرة وضعت لمجابهة الجرائم التقليدية ذات الطابع المادي و التي تخلف ورائها أثارا مادية محسوسة ، و لم تتناول في صلب نصوصها الجرائم المعلوماتية ، هذه الأخيرة التي لا ينفك معدل

إنتشارها عن الإرتفاع و تتزايد يوما بعد يوم ، و ذلك بفعل عجز السلطات المختصة بتنفيذ القانون عن مجابهتها بسبب عدم ملائمة النصوص الإجرائية لطبيعتها الخاصة ، فالنصوص الخاصة بالبحث و التحقيق في مجال الجرائم التقليدية لا تصلح للتطبيق في مجال الجرائم المعلوماتية ، فالنصوص المتعلقة بإصدار اوامر القبض و الإحضار و على سبيل المثال لا يمكنها أن تجدي نفعا في مواجهة مجرمي المعلوماتية الذين قد يرتكبون فعلهم الإجرامي من نقطة تقع في أقصى بقاع الأرض ، و ذلك بسبب عائق مبدأ إقليمية النص الجنائي ، و هو ما يتسبب في شل أيدي العدالة عن ممارسة أعمال البحث و التحقيق بشأن الجرائم المعلوماتية ، و قد تتم في بعض الأحيان تحت طابع الضرورة و الإستعجال مباشرة الإجراءات بالرغم من عدم توافقها مما قد يتسبب في إهدار حقوق الغير بفعل تعسف السلطات المختصة في تطبيق إجراءات غير منصوص عليها قانونا تخت غطاء ضرورات التحقيق و الحفاظ على الأدلة .

إن واقع الحال يدل على صراع خفي بين مجرمي المعلوماتية و السلطة المختصة بأعمال البحث و التحقيق الجنائي ، فأولئك يعملون بشكل دائم و متناسق مع تطور التكنولوجيا المعلوماتية ، من خلال وضع و رسم خطط إجرامية مستقبلية ، تضمن عدم إكتشاف امر جرائمهم أو تجعل من امر تتبع اثارهم أمرا بالغا في الصعوبة و التعقيد ، إن لم نقل امرا مستحيلا من خلال إعتمادهم أساليب إجرامية مستحدثة في عالم تكنولوجيا المعلومات ، يقابله في ذلك جهود دائمة من قبل الهيئة التشريعية و جهات البحث و التحقيق من أجل مسايرة هذا النسق ، و الإحاطة بكل ما هو مستجد في فضاء المعلوماتية و مجالها الإجرامي ، و ذلك من خلال رسم و العمل على تجسيد سياسة مكافحة الجرائم المعلوماتية بشكل فعال اساسها الشرعية الإجرائية، من خلال إستحداث نصوص قانونية إجرائية ملائمة وفعالة لمواجهة هذا النوع من الجرائم و المجرمين ، إضافة إلى تطوير عامل الإمكانيات المادية و البشرية المؤهلة لتجسيد هذا الغرض ، من خلال تخصيص وحدات مختصة بمباشرة أعمال البحث و التحقيق في الجرائم المعلوماتية

دون سواها ، تجتمع لديهم السلطة القانونية و الخبرة و المعرفة اللازمة بمجال النظم و الجرائم المعلوماتية ، و هو ما يسمح لهم بتخطي العقبات التي يواجهونها في إطار أداء مهامهم و تحقيق الأهداف المنشودة من كل ذلك و هي فك شفرة الجريمة المعلوماتية و وضع مرتكبها في مواجهة العدالة .

إن موضوع الدراسة موضوع متسع النطاق يجمع بين الجانب التقني لعالم المعلوماتية ، و الجانب القانوني المتمثل في الجريمة المعلوماتية ذاتها، و الشق الإجرائي المتعلق بأعمال بالبحث و التحقيق الموجهة للكشف عنها ، غير أن دراستنا تهدف و في ظل تعدد المعطيات إلى تسليط الضوء على الجانب القانوني الإجرائي خصوصا المتعلق بأعمال البحث و التحقيق بشأن الجرائم المعلوماتية ، مع عدم إقصاء الجانب الموضوعي و التقني للجريمة المعلوماتية ، نظرا لكون الموضوع نقطة تقاطع بين عالم تكنولوجيا المعلومات و القانون .

ثانيا – أهمية الموضوع و أسباب إختياره.

يستمد موضوع البحث أهميته من عدة جوانب تبرر أسباب إختياره تظهر من خلال :

1– التزايد المستمر للنشاط الإجرامي عبر النظم المعلوماتية ، و تزايد درجة خطورة هذا النشاط و إرتفاع مستوى التهديدات التي يشكلها على الأمن العام ، في ظل الإعتماد المطلق على تكنولوجيا المعلومات في المجتمعات المعاصرة ، يقابله عجز سلطات البحث و التحقيق عن رسم نموذج موحد لهذه الجرائم و الإستقرار على جملة من الإجراءات الخاصة بمتابعتها نظرا لتطورها الدائم و المستمر ، مما ينتج عنه أحيانا غياب أو جمود النص الإجرائي و عجزه عن تفعيل الإجراءات بسبب عدم ملائمته للجريمة محل البحث و التحقيق.

2– تصنيف موضوع إجراءات البحث و التحقيق بشأن الجرائم المعلوماتية من بين اهم المواضيع المطروحة للنقاش على النطاق الدولي و الوطني ، فهي تشغل بإستمرار حيزا مهما من جهود الباحثين

و كذلك الفقه و التشريع لأجل وضع إستراتيجيات قانونية و عملية آنية و مستقبلية، تضمن عدم فقدان السيطرة على تقنية المعلوماتية ، و تحولها من تقنية تساعد على تطور المجتمعات من خلال تبادل المعارف و المعلومات إلى تقنية هدامة .

3- الرغبة في التعمق في دراسة و تحليل الآليات القانونية الإجرائية الحديثة الموجهة لمكافحة النشاط الإجرامي الإلكتروني ، و التي أسست لها الجهود و المعاهدات الدولية والإقليمية كإتفاقية بودابست لمكافحة الجرائم المعلوماتية ،و الإتفاقية العربية لمكافحة الجرائم المتصلة بتقنية المعلوماتية ، و كذلك الجهود التشريعية الداخلية ، كما هو عليه الحال في الجزائر التي أقرت بتشريع خاص يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها، وذلك بتاريخ 05 أوت 2009 بموجب القانون رقم 09-04 ، و هي القوانين التي تحاول تنظيم فضاء المعلوماتية بصفة عامة ، و مكافحة الجانب الإجرامي المتصل بها ، من خلال تحديد قواعد إجرائية خاصة تسمح بمتابعة هذا النوع من الجرائم و مرتكبيها بشكل يضمن شرعية الإجراءات المتخذة ، بهدف ردع هذه الفئة من المجرمين التي دأبت على تبني منطق الإفلات من العقاب ، بحجة قدرتهم على تعطيل الإجراءات من خلال إعتمادهم على وسائل و أساليب إلكترونية إجرامية غاية في التعقيد من الناحية التقنية ، تجعل من أمر تحصيل الأدلة الإلكترونية في مواجهتهم امرا بالغا في الصعوبة ، نظرا لتسببها في تعطيل النصوص الإجرائية بسبب طابع اللاملائمة بين الإجراءات و طبيعة الجرائم.

4- إن موضوع البحث يكتسي أهمية بالغة من الناحية العملية ، فمبرر غياب النصوص الملائمة لمباشرة الإجراءات قد لا يكون السبب الوحيد في ظهور إشكالات متعلقة بإجراءات البحث و التحقيق في مجال الجرائم المعلوماتية ، فقد تتوفر النصوص القانونية المناسبة و تغيب الوسائل المادية الضرورية لتنفيذ الأعمال الخاصة بالبحث و التحقيق ،و قد يحدث ان يتوفرا معا و لكن تغيب المهارة و المعرفة الفنية لدى

رجال البحث و التحقيق، و هي كلها عوامل تستقطب الإهتمام لأجل معالجتها بالبحث و التحليل لأجل الوصول إلى وضع تصور قانوني و فني في آن واحد ، يضمن التعريف بموضوع الجريمة المعلوماتية بشقيها المعلوماتي و الإجرامي و الإجرائي .

إن أهمية الموضوع و أهدافه و على إتساع نطاقها تبرر أسباب إختياره و تجعل منه موضوعا مستجدا و مستحدثا للدراسة و البحث بشكل دائم و مستمر، بالنظر إلى نطاق المعلوماتية الذي لا ينفك يتوسع من يوم لآخر ،إضافة إلى تطورها بشكل دائم ومستمر و عدم وجود عوائق تحد من هذا التطور ،و هو ما يجعل من امر تطوير و تحديث النصوص القانونية الإجرائية أمرا واجبا في ظل التهديدات التي تشكلها الجريمة المعلوماتية.

ثالثا : صعوبات البحث.

إن الوصول إلى وضع خطة متوازنة و معالجة فعالة و دقيقة لموضوع البحث لم يكن بالسهولة المتوقعة بدءا، بالنظر إلى طبيعة الموضوع المزدوجة (القانونية و الفنية)، و التي شكلت تحديا بالغ الصعوبة نظرا لما يميز الموضوع من دقة المصطلحات و المفاهيم العلمية منها و القانونية ، و التي يصعب التحكم فيها و توظيفها بشكل متناسب و متلازم، مع مراعاة عدم تغليب أي من الطابع القانوني على الفني أو العكس من ذلك ، تحت طائلة فقدان البحث لمعالمه المزدوجة.

إضافة إلى مجموعة من الصعوبات الأخرى التي يمكن ذكرها بإيجاز :

- قلة الدراسات السابقة في المجال الإجرائي و إتجاه أغلبها لمعالجة الظاهرة الإجرامية المعلوماتية من ناحية السلوك الإجرامي و العقوبات المقررة لها ، دون التركيز على الجانب الإجرائي ، و هو ما جعل الباحث امام حتمية تجميع المعلومات الخاصة بالموضوع في شكل جزئي و إعادة تجميعها بشكل متناسق وفق خطة عمل ذاتية.

- بعد مجتمع الباحث عن موضوع البحث و عدم إلمامه بحيثياته و أبعاده ، مما جعل الباحث يبحث بصفة إنفرادية ضمن فضاء لا محدود من المعلومات الخاصة بالجرائم المعلوماتية ، وما يميزها من لغة خاصة متميزة تُصعب أحيانا فهم بعض الجزئيات الخاصة بالموضوع ، خصوصا ما شكل منها نقطة تلاقي بين المعلوماتية و القانون.
- إنعدام قنوات التواصل مع الجهات الأمنية و القضائية التي تختص بمتابعة أعمال البحث و التحقيق في الجرائم المعلوماتية ، مما تسبب في خلو بعض مواضع البحث من الإحصائيات الضرورية الخاصة بواقع الحال على المستوى الوطني ، و كذلك للوقائع الحية و التي كانت ستساهم بشكل أفضل في توضيح أفكار البحث.

رابعا: إشكالية الموضوع.

إن التغيير الحاصل على مستوى النشاط الإجرامي بفعل إتصاله بتقنية المعلوماتية، صاحبه تحول كبير على المستوى القانوني و بالخصوص الإجرائي ، فظهرت آليات و إجراءات قانونية مستحدثة في مجال البحث و التحقيق ، أساسها النص القانوني ، و ميدانها الجرائم المعلوماتية ، غير أن تطور كلا المجالين لا يسري بنفس الوتيرة ، فالجرائم المعلوماتية تتطور بشكل سريع و مذهل ، فيما تعرف النصوص و الإجراءات القانونية وتيرة بطيئة من حيث مسايرتها لواقع الجريمة المعلوماتية ، مما يخلق دوما فجوة بين الجريمة و الإجراءات الموضوعة لمتابعتها قد تتسبب في تعطيل أو شَل عمل الجهات المختصة بمباشرة هذه الإجراءات، و ذلك بالرغم من الجهود التشريعية المبذولة على الدوام لأجل تسخير أفضل الإجراءات الكفيلة بتسهيل إجراءات البحث و التحقيق في الجرائم المعلوماتية، إن الواقع المميز للجريمة المعلوماتية و أثارها على القوانين الإجرائية الجزائية هو ما دفعنا إلى معالجة هذا الموضوع بالبحث ، خصوصا في ظل غياب دراسات سابقة على هذا المستوى متعلقة بالموضوع ، و قد وضعنا في

سبيل تحقيق ذلك إشكالية متناسبة و موضوع البحث و هي الإشكالية التي يمكن صياغتها في صلب التساؤل التالي :

ما مدى فعالية الآليات القانونية المستحدثة في مجال دعم أعمال البحث و التحقيق للكشف عن الجرائم المعلوماتية؟

وتندرج تحت هذه الإشكالية الرئيسية مجموعة من التساؤلات الفرعية المتوافقة و تسلسل أفكار البحث و التي يمكننا إيجازها في جملة التساؤلات التالية :

1. ما المقصود بتقنية المعلوماتية و ما هي إنعكاساتها الإجرامية؟
2. هل هناك جهود على مستوى الفقه و القانون تهدف إلى دعم أعمال البحث و التحقيق بشأن الجريمة المعلوماتية؟
3. ما هي الخطط العملية و السياسات المنتهجة الدولية منها و الداخلية ، الهادفة إلى ضمان حسن سير الإجراءات الخاصة بالبحث و التحقيق في الجرائم المعلوماتية ؟
4. هل تخضع إجراءات البحث و التحقيق في الجرائم المعلوماتية لإختصاص رجال إنفاذ القانون العاديين ، أم لفرق متخصصة تمتلك من القدرات و الوسائل الملائمة لطبيعة الجريمة المعلوماتية؟
5. ما هي طبيعة الأدلة المستهدف تحصيلها من خلال أعمال البحث و التحقيق في الجرائم المعلوماتية؟

إن كل هذا الطرح سواء الإشكالية الرئيسية او مجموعة التساؤلات الفرعية لا يدل سوى على مدى عمق الموضوع و تشعبه، نظرا لكونه موضوعا يجمع بين مجالين متباعدين نظريا و هما مجال تكنولوجيا المعلومات و مجال القانون ، و هو ما سنحاول تقريبه بالإجابة من خلال أطوار البحث على كل التساؤلات المطروحة مسبقا .

خامسا- منهج و خطة البحث .

إن البحث في مجال الإجراءات الخاصة بالبحث و التحقيق في مجال الجرائم المعلوماتية ، يفرض على الباحث إعتماد منهجية علمية خاصة تتماشى و ترتيب الأفكار المطروحة للنقاش حسب خطة البحث ، و لذلك فقد إعتمدنا مناهج بحثية متعددة بدرجات متفاوتة من حيث الأهمية ، إعتلى صدارتها المنهج الوصفي و كذلك التحليلي ، من خلال ما ورد في البحث من وصف لمفهوم النظم المعلوماتية و الجريمة المعلوماتية ، و مختلف الجهود الفقهية و القانونية المتعلقة بمسألة البحث و التحقيق في الجرائم المعلوماتية ، إضافة إلى التعرض لمختلف الجهات المختصة بمباشرة هذه الإجراءات و وسائلها و أساليب عملها ، وصولا إلى نتاج هذه الأعمال و الإجراءات ، و كل ذلك في شكل وصف دقيق مصحوب بالتحليل القانوني لأجل الكشف عن مواطن اللبس التي تعتري موضوعنا المتسم بطابعه الإجرائي الدقيق ، إضافة لذلك فقد كان للمنهج المقارن نصيب وافر من الإستعمال بوصفه منهجا مساعدا بالدرجة الأولى ، بحيث إستعنا به خلال كامل أطوار البحث لأجل وضع نتائج من خلال المقارنة بين مختلف الأنظمة و التشريعات التي أولت أهمية قصوى لموضوع إجراءات البحث و التحقيق في مجال الجرائم المعلوماتية ، و هي المناهج البحثية التي ساعدتنا في الوصول إلى مجموعة من النتائج الدقيقة و التي إستعرضناها تبعا وفق ثلاث (03) فصول رئيسية ، فرضتها علينا طبيعة الموضوع و التي قادتنا إلى الخروج عما ألفناه من تقسيمات ثنائية ، بحيث و ردت فصولنا الثلاث موسومة بعناوين مختارة حسب التقسيم التالي:

- ✓ **الفصل الأول: مفهوم الجريمة المعلوماتية.**
- ✓ **الفصل الثاني : شرعية إجراءات البحث و التحقيق في الجرائم المعلوماتية و الجهات المختصة بتنفيذها.**
- ✓ **الفصل الثالث: الإجراءات الخاصة بالبحث و التحقيق في الجرائم المعلوماتية و آثاره.**

الفصل الأول

الإطار المفاهيمي للجريمة المعلوماتية

إعتمد الإنسان منذ القدم في نقل المعلومات بشتى أنواعها ، على مختلف الوسائل كالرسومات و الكتابة على الأحجار و جلود الحيوان و الورق ، و كل ذلك بغرض حفظ هذه المعلومات و تخزينها و تسهيل أمر إسترجاعها ، لأجل مواجهة وضعية مستعصية تحتاج إلى كم من المعلومات تشكل حلا لها ، و تعتبر الكتب و المخطوطات و الوثائق و المستندات، من أهم مصادر نقل المعلومة التي إعتمدها الإنسان في العهد القريب ، غير انه تخلى عنها في الوقت الحاضر بفعل ما وفرته له تقنية المعلوماتية في مجال التعامل مع المعلومة ، سواء من حيث نقلها أو تحزينها أو إسترجاعها بل حتى إستعمالها للتنبؤ بما قد يحدث مستقبلا ، و ذلك من خلال إنتشار الحواسيب على أعلى نطاق ، و ظهور تقنيات حديثة لتبادل المعلومات و للإتصال في شكل شبكة المعلومات الدولية(The Web) و شبكة الأنترنت ، كل ذلك خلق جانبا مشرقا تمثل في تحسين و تيسير عمل الدول و الحكومات و المؤسسات في مجال التعامل فيما بينها ، أو مع المجتمعات التي تحكمها و تتعامل معها ، كما ساهمت هذه التقنية في تطور نمط حياة الإنسان الذي أصبح يعتمد بشكل شبه كامل على الحواسيب و شبكات الإتصال و تبادل المعلومات لأجل قضاء حوائجه دون عناء التنقل من مكان لآخر سعيا وراء المعلومة أو المرفق ، غير انه و بالموازاة مع ذلك ظهر جانب مظلم لهذه التقنية تمثل في سوء تسخير مزاياها لأجل الإعتداء على مصالح الغير المتمثلة في جملة المعلومات ذات الطابع المتاح او السري المتداولة عبر النظم المعلوماتية من خلال الحواسيب و الشبكات ، و ذلك من قبل فئة أصطلح عليها وصف " مجرمي المعلوماتية " ، لا لسبب سوى لأنهم يحملون و يعبرون عن ميول إجرامي لا يقل خطورة عن باقي المجرمين التقليدين من فئة القتلة او اللصوص و المحتالين ، و يرتكبون أفعالا مجرمة قانونا و معاقب عليها بعقوبات قد تكون أشد مما قد يتصوره البعض منا ، بهدف تحصيل مكتسبات ذات طابع معنوي في شكل معلومات و بيانات لا يدرك قيمتها إلا مالكها أحيانا و مجرمو المعلوماتية ، إن ظهور هذا النوع المستحدث من الجرائم الناتج عن إتصال عالم تكنولوجيا المعلومات بالقانون ولد مفاهيم من نوع خاص كانت محل إهتمام قانوني ، بهدف ظبطها لأجل تيسير عمل الجهات المختصة بمباشرة الإجراءات الخاصة بالبحث و التحقيق

بشأن الجرائم المعلوماتية، و هي المفاهيم التي لا يمكن إنكارها و تجاوزها في مجال دراستنا بإعتبارها من أساسيات الموضوع ، و من أجل ذلك فقد خصصنا الفصل الأول كفضاء مفاهيمي لبناء الأفكار حول موضوع تقنية المعلوماتية و الجريمة المعلوماتية أولا و قبل كل شيء ، و ذلك من خلال الإجابة على التساؤل التالي : ما هو المفهوم المحدد للجريمة المعلوماتية من الناحية التقنية و في ظل أحكام القانون الجنائي ؟

إن الإجابة عن كل ذلك توجب علينا تقسيم فصلنا هذا إلى مبحثين:

- **المبحث الأول المعنون بـ: الإطار المفاهيمي للجريمة المعلوماتية .**
- **المبحث الثاني تحت عنوان: صور الجريمة المعلوماتية.**

و هما المبحثان اللذان حولنا فيهما توضيح الجانب الخاص و التقني للجريمة المعلوماتية و المتمثل في النظم المعلوماتية و ما يلحق بها من مفاهيم علمية ، ثم إستغلال مكتسباته العلمية في توضيح الجانب القانوني للجريمة المعلوماتية على إعتبار أنهما وجهان لعملة واحدة ، كل ذلك بغرض خلق تناسق بين خصوصيات الجريمة المعلوماتية و وسائل البحث و التحقيق الخاصة و التي سنستعرضها لاحقا .

المبحث الأول : مفهوم الجريمة المعلوماتية .

غالبا ما تستهدف الجريمة بوصفها فعلا محظورا بموجب نصوص القانون العقابية حقوق الغير ، فنجد منها ما يستهدف المال أو الشخص في حد ذاته سواء بكيانه المادي او المعنوي ، غير انه و في ظل المتغيرات الاجتماعية التي تحمل في طياتها مفاهيم الحداثة و التطور التكنولوجي ، و التي غيرت من نمط معيشة الإنسان إلى ما هو افضل و من كافة النواحي كل ذلك بفضل التقنيات التكنولوجية التي توفرها، ظهر نوع جديد من الجرائم يستهدف المال و النفس من خلال الفضاء الرقمي الإلكتروني ، كنتيجة لإنتشار تقنية المعلوماتية التي أضحت تشكل عصب الحياة الحديثة و نقطة قوة في مسار التقدم الحضاري لأي دولة كانت ، فبدونها لا تستطيع أي دولة إحراز التقدم المرجو و اللحاق بركب المجتمع الدولي[1] ، فقد أصبح تبادل المعلومات و معالجتها بأسرع وقت و أفضل طريقة الشغل الشاغل لاختصاصي هذا المجال بالرغم من درجة التطور و التقدم التي آلت إليها هذه التكنولوجيا ، غير ان هذا الإهتمام كان محل فئة أخرى و هي فئة المجرمين الذين أصروا على إقتحام هذا المجال من خلال الإعتداء على الأنظمة المعلوماتية بأهداف متباينة ، منها ما يهدف إلى إثبات الذات و التحدي ، ومنها ما يهدف إلى تحقيق ثروة على حساب الغير ، و منها ما يهدف إلى أبعد من ذلك من خلال المساس بأمن و سلامة الفرد و المجتمع ، و هي الظاهرة التي أصطلح عليها تسميتها " الجريمة المعلوماتية " La Cybercriminalité، هذه الجريمة التي أصبحت تشغل فكر القانونين ،

---

[1]– حسب التقرير الإحصائي السنوي للواقع الرقمي حول العالم لسنة 2014 ، فإن عدد سكان الأرض الذين يستخدمون تقنية الأنترنت قد بلغ 2.484.915.152 مليار نسمة من مجموع 7.095.467.818 مليار نسمة ، أي بمعدل 35% من سكان المعمورة ، بينما يستخدم ما مجموعه 1,856,680,860 مليار نسمة من سكان الأرض مواقع التواصل الإجتماعي بشكل دائم في حياتهم اليومية بمعدل 26%، أما عدد سكان الأرض الذين يستخدمون تقنية الهاتف النقال فقد بلغ 6,572,950,124 مليار نسمة أي بمعدل 93%. أنظر في ذلك: The Global Digital Statistic 2014– p 05.

متوفر على شبكة الأنترنت - تاريخ التصفح: 2015/01/05 - الرابط الإلكتروني:

http://etonpreneurs.com/uploads/Global%20Social,%20Digital%20&%20Mobile%20Statistics,%20Jan%202014.pdf

و المعلوماتيين ، و السياسيين و قادة الدول و الحكومات ، نظرا لما تشكله من تهديد فعلي على أمن الجماعة و الفرد ، بفعل خصوصية محلها و المتمثل في جملة المعطيات و البيانات الرقمية المعلوماتية ذات الطبيعة الخاصة و المميزة جدا من حيث أهميتها.[1]

فما هي يا ترى طبيعة هذه المعلومات و لما تشكل محل إهتمام بالغ و مزدوج من قبل القائمين على أمنها و كذلك المجرمين ؟ و ما هي أبعاد الجريمة المعلوماتية من ناحية مفهومها القانوني ؟ و من هو المجرم المعلوماتي؟ و للإجابة عن هذا التساؤل الفرعي كان من الضروري التعرض لمفهوم المعلوماتية بدءأ (المطلب الأول) ، و لظاهرة الجريمة المعلوماتية بعد ذلك (المطلب الثاني) ، و لخصائص المجرم المعلوماتي و الضحية أخيرا (المطلب الثالث).

المطلب الأول : مفهوم النظم المعلوماتية.

تعتبر المعلومات الهدف الرئيسي للجريمة المعلوماتية باعتبارها محلها الرئيسي ، فلا يتاح للمجرمين المعلوماتيين الوصول إليها إلا من خلال منفذ وحيد و هو النظام المعلوماتي Le Système Informatique الذي يشكل الوعاء المنطقي لها ، و الذي أنشأ خصيصا بغرض تداولها و فق نظم معالجة آلية تتحكم فيه أجهزة الحاسوب ، منفردة او مجتمعة بواسطة الربط بشبكات الإتصال ، تعمل على تداول و معالجة المعلومات بأفضل و أسرع طريقة ممكنة بهدف ترقية الأداء المؤسساتي لأجهزة الدولة ، و مصالحها الحيوية كالدفاع و الصحة و التعليم و الإعلام...إلـخ ، ضف إلى ذلك تيسير المعاملات بين الأفراد داخل المجتمع ، من خلال تقديم خدمات ذات طابع إلكتروني كالبيع و الشراء و الدفع الإلكتروني ، أو خدمات البريد الإلكتروني ، و ما يجاورها

---

[1]– قدر عدد الجرائم المعلوماتية المرتكبة في فرنسا سنة 2012 من قبل مصالح الشرطة و الدرك بـ: 84,774 ألف جريمة معلوماتية. أنظر في ذلك : تقرير مجموعة العمل الحكومية المشتركة الفرنسية تحت عنوان – حماية مستعملي شبكة الأنترنت– فيفري 2014– ص 22– متوفر على الموقع الرسمي لوزارة العدل الفرنسية – تاريخ التصفح: 2015/03/05- الرابط الإلكتروني: http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf

من خدمات تستلزم الإدلاء بمعلومات شخصية ذات طابع سري ، مما يجعل من هذه النظم المعلوماتية هدفا يستقطب هواة و محترفي الإجرام المعلوماتي على حد سواء ، و لكن و قبل التطرق إلى الجانب الموضوعي المتعلق بطبيعة الجريمة المعلوماتية وجب علينا بدءاً التعريف بالنظم المعلوماتية أساسا ، هذه العبارة التي تظل تتردد على مسامعنا بشكل دائم و مستمر و التي تشكل عنصرا هاما من عناصر حياتنا اليومية ، فما هو يا ترى مدلول " المعلوماتية " و " النظم المعلوماتية " من الناحية التقنية و القانونية ؟

إن الإجابة عن هذا التساؤل تقتضي منا تحديد مفهوم المعلوماتية أولا و بيان مدى أهميتها (الفرع الأول)، إضافة إلى تحديد أبعادها و مجالات استخداماتها ثانيا (الفرع الثاني) ، مع التعرض إلى الجانب التشريعي الذي اولى لهذه المسائل أهمية بالغة من حيث توفرها على قدر عالي من الحماية الجنائية ضمانا لأمنها و سلامتها.

الفرع الأول: تعريف المعلوماتية .

أسهمت التطورات التكنولوجية و التقنية المتسارعة في نهاية القرن العشرين و بدايات القرن الواحد و العشرين ، في سرعة تحول المجتمعات من عصر الصناعة إلى عصر المعلومات ، و تحولت أساليب و انشطة العمل تدريجيا إلى النمط الإلكتروني بفضل التمازج بين تقنيتي الإتصالات و المعلومات مما أسفر عن إنطلاقة قوية في عالم تقنية المعلومات ، كان نتاجها ظهور تطبيقات حضرية ذات طابع تقني كالحكومة الإلكترونية ، التجارة الإلكترونية ، و ذلك بإعتبارها الجانب الإيجابي للتطور التكنولوجي المعاصر ، أما الجانب السلبي المرافق لها فقد تجلى في ظهور الجرائم المعلوماتية كنتيجة حتمية لإساءة إستخدام هذه التقنيات .[1]

[1]– عبد الله بن سعود محمد السراني – فعالية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني– رسالة مقدمة لأجل نيل شهادة الدكتوراه قسم العلوم الشرطية – جامعة نايف للعلوم الأمنية – الرياض – السعودية – سنة 2009– ص 21.

إن الاستخدامات اللامتناهية لتقنية المعلوماتية نتيجة شيوع إستعمال الحواسيب ، و الهواتف الذكية المتصل أغلبها بشبكة الأنترنت، و ذلك على كل المستويات الحكومية منها والخاصة جعل من أمر تداول المعلومات أمرا محفوفا بالمخاطر، بالنظر إلى حجم التهديدات التي تشكلها الجريمة المعلوماتية على أمنها ، في شكل تلك المعلومات التي تخص المصالح الأمنية و الدفاعية للدول او تلك المتعلقة بالبيانات المالية او الشخصية ، و بالتالي فإن موضوع الأمن المعلوماتي المنصب على مسائل تامين النظم المعلوماتية بما تتضمنه من معلومات أضحى من المواضيع التي تحظى بالإهتمام التشريعي و القانوني ، لأجل تأمين هذا المجال الحيوي و ضمان سياسة وقائية دفاعية ضد هواة و محترفي الإجرام المعلوماتي ، و لكن و قبل ولوج النقاش القانوني وجب علينا بدءاً تعريف المعلوماتية إنطلاقا من أبسط جزئياتها ألا و هي المعلومات ، ثم تقنية المعلوماتية ، و في الأخير النظم المعلوماتية.[1]

الفقرة الأولـــــى : تعريف المعلومات .

أن نتطرق لموضوع وسائل التحقيق في الجرائم المعلوماتية يقتضي و بالضرورة ان نعرف بأحد أهم جزئيات الموضوع ألا و هو المعلومات ، هذه العبارة التي شاع إستعمالها في الأونة الأخيرة و شاعت إستعمالاتها في شتى مجالات حياتنا اليومية تدفعنا للتساؤل حول طبيعتها ومدى اهميتها في نطاق بحثنا؟

أولا : التعريف اللغوي : أشتق مصطلح " المعلومات " لغة من كلمة "علم" و دلالتها هي المعرفة التي يمكن نقلها و إكتسابها، و أصلها في اللغة الفرنسية و الإنجليزية و الألمانية و الروسية هو كلمة Informolio

[1] – يقضي متوسط الفرد الواحد البرازيلي يوميا ما مقداره 6,1 ساعة على شبكة الأنترنت من خلال الحاسوب ، و ما مقداره 2,4 ساعة موصولا بالشبكة بواسطة الهاتف الذكي و هو اعلى معدل على الصعيد الدولي ، أما على المستوى العربي فالفرد الإماراتي هو الأول عربيا و السابع عالميا من خلال قضاءه 5,2 ساعة موصولا بالشبكة بواسطة الحاسوب ، و 3 ساعات بواسطة الهاتف الذكي . أنظر في ذلك: The Global Digital Statistic 2014– op cit – p 31.

اللاتينية بحسب الأصل و الدالة على شيء للإبلاغ و التوضيح ، و قد وصفها عالم الرياضيات الأميركي "كلود شانون" "Claude Chanone" بأنها " إختزال اللاتحدد ".

ثانيا: التعريف الإصطلاحي: ، لقد أشار عديد الباحثين بإختلاف تخصصاتهم إلى تعريف إصطلاحي للمعلومات يمكن جمعها في مفهوم يقصد به " الحقائق أو الرسائل أو الإشارات أو المفاهيم التي تعرض بطريقة صالحة للإبلاغ أو التوصيل أو التفسير بواسطة الإنسان او ادوات و معدات آلية" ، أو بأنها " الصورة المحولة للبيانات و قد تم تنظيمها و معالجتها بطريقة تسمح بإستخلاص النتائج".[1]

ثالثا : التعريف القانوني : إهتم جزء قليل من التشريعات بوضع تعريف للمعلومات و في سبيل ذلك نذكرما جاء به المشرع الفرنسي و فق ما يقرره القانون رقم 82-652 الصادر في 1982/07/26 الخاص بتنظيم الإتصالات السمعية و البصرية بأنها " رنين صور الوثائق و البيانات و الرسائل أيا كانت طبيعتها".[2]

ليلحق به المشرع الأمريكي بموجب القانون الصادر سنة 1999 المنظم للمعاملات التجارية الإلكترونية بالقول في الفقرة 10 من المادة 02 بان المعلومات هي " كل البيانات و الكلمات و الصور و الأصوات و الوسائل و برامج الكمبيوتر و البرامج المضغوطة سواء على أقراص مرنة أو قواعد بيانات أو ما شابه ذلك " و بذلك فقد أكسب المشرع الأمريكي الطابع التكنولوجي لمدلول كلمة " معلومة" و هو ما أخذ به كلا من التشريعين البحريني و الإماراتي، اللذان نصا على تعريف مشترك من حيث المفهوم بموجب القانونين الصادرين تبعا سنة 2002 المتعلقين بتنظيم المعاملات الإلكترونية ، بالقول بان المعلومات هي " معلومات ذات

---

[1] – محمد علي العريان – الجرائم المعلوماتية – دار الجامعة الجديدة – الإسكندرية– مصر – 2004– ص35،36.

[2]- المرجع السابق – ص 39.

خصائص إلكترونية في شكل نصوص أو رموز أو أصوات أو رسوم أو صور أو برامج حاسب ألي أو غيرها من قواعد البيانات ".[1]

و ما يمكن الإشارة إليه هو تعريف المشرع الجزائري الوارد في نص المادة 02 الفقرة "ج" من القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها، بالقول بأن المعطيات المعلوماتية هي " أي عملية عرض للوقائع و المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج التي تجعل من المنظومة المعلوماتية تؤدي وظيفتها" إن تعريف المشرع الجزائري يتسم بالعمومية المبالغ فيها فهو تعريف يبتعد عن الدقة في ميدان تعريف المعلومة بالخصوص و عليه وجب إعادة صياغة تعريف المعلومة من اجل فصل مفهومها عن باقي المفاهيم الأخرى ، خصوصا و ان ميدان المعلوماتية دقيق لا يحتمل الخلط بين المفاهيم.[2]

رابعا: أنواع المعلومات. تقسم المعلومات إلى ثلاث (03) طوائف و هي :

1. المعلومات الإسمية : و التي تتضمن المعلومات المرتبطة بشخص معين كإسمه موطنه، حالته الإجتماعية و هي كلها معلومات سرية لا يجوز الإطلاع عليها إلا بموافقته.
2. المعلومات المتعلقة بالمصنفات الفكرية: و هي المعلومات الفكرية و هي محمية بموجب قوانين حماية الملكية الفكرية يضاف إليها المعلومات المتعلقة بالاختراعات و التسجيلات الفنية.
3. المعلومات المتاحة : و هي تلك المعلومات المتاحة للجميع مثل تقارير البورصة و النشرات الجوية .[3]

---

[1]- عبد العال الدريبي – الجرائم الإلكترونية – دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية و الأنترنت – المركز القومي للإصدارات القانونية – القاهرة – مصر – 2012- ص 44.

[2]- القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها، المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية رقم : 47 ، الصادرة بتاريخ : 16 أوت 2009- طالع الملحق رقم : **02.**

[3]- عبد العال الدريبي – مرجع سابق – ص 45.

خامسا: شروط الحماية القانونية للمعلومات: لكي تكون المعلومة محل حماية قانونية يجب أن تتوفر فيها الشروط التالية:

1- **أن تكون المعلومة محددة ومبتكرة** : يجب ان تتسم المعلومة بالتحديد أي أن يتم حصرها في نطاق معين، و قد ذهب البعض في ذلك بالقول كالأستاذ "كاتالا" Catala " إن المعلومة و قبل كل شيء تعبير و صياغة مخصصة من أجل تبليغ رسالة عن طريق علامات أو إشارات مختارة " ، ضف إلى ذلك فيجب ان تكون المعلومة مبتكرة و أصيلة أي غير موجودة سابقا، و بذلك تستثنى من نطاق المعلومات الشائعة السهل الوصول إليها لعدم إرتباطها بشخص معين.[1]

2- ان تكون المعلومة مستأثرا بها و سرية : يشترط صفة السرية في المعلومة لتكون محل الحماية القانونية، و تكتسب المعلومة صفة السرية إما بالنظر إلى طبيعتها أو إلى إرادة الشخص كأن يحيطها برقم سري مثلا.[2]

الفقرة الثانية : تعريف تقنية المعلوماتية – L'informatique

نظرا للإنتشار الواسع للمعلومات و تمركزها في لب دورة التطور الحضاري ، من خلال اتساع دائرة الإهتمام المتعلق بإنشاء نظم تعمل على أوسع نطاق و بأسرع طريقة ممكنة، من أجل تخزين و تداول المعلومات مع ضمان فعاليتها ضمن مجال إستخداماتها كالدفاع و الصحة و التعليم و القضاء ، ظهر ما يعرف بتقنية المعلوماتية L'informatique .

يمكن القول بان المعلوماتية ظاهرة إجتماعية ذات بعد تاريخي نشأت و تطورت مع تطور الحضارة ، و يرجع الفضل في إقتراح مصطلح المعلوماتية إلى العالم الفرنسي " دريفيس" Dréfus ، الذي إستخدمه اول مرة سنة 1962 ، لتمييز المعالجة الآلية للمعلومات عن غيرها من أنظمة معالجة المعلومات.[3]

---

[1]- محمد علي العريان– مرجع سابق – ص 38.

[2]- عبد العال الدريبي – مرجع سابق – ص 45.

[3]- تركي بن عبد الرحمان المويشير- بناء نموذج أمني لمكافحة الجرائم المعلوماتية و قياس فعاليته- رسالة مقدمة لأجل نيل شهادة الدكتوراه- قسم العلوم الشرطية – جامعة نايف للعلوم الأمنية – الرياض – السعودية – 2009- ص 14.

و قد كان للأكاديمية الفرنسية نصيب في وضع تعريف للمعلوماتية حسب ما ورد في مقرر جلستها المنعقدة في 02 أفريل 1967 بالقول بأنها " العلم التفاعلي العقلاني بواسطة آلات أوتوماتيكية مع المعلومات بإعتبارها دعامة للمعارف الإنسانية و عماداً للإتصالات في ميادين التقنية الإقتصاد والإجتماع ".[1]

و لعل أن التعريف الأكثر تداولا لمدلول المعلوماتية L'informatique ، هو ذلك الذي عرفها بأنها " علم يعنى بالموضوعات و المعارف المتصلة بأصل المعلومات و تجميعها و تنظيمها ، و إختزانها و إسترجاعها و تفسيرها و بثها و تحويلها و إستخدامها ، كما يتضمن البحث عن تمثيل المعلومات في النظم الطبيعية و الصناعية و الإدارية ، و إستخدام تقنيات الترميز في نقل الرسالة و التعبير عنها ، إضافة إلى الإهتمام بأساليب معالجة المعلومات كالنظم المعلوماتية و نظم البرمجة " و يمكن تلخيص ذلك بالقول بأن المعلوماتية هي " المعالجة الآلية للمعلومات ".[2]

إذن و بإعتبار المعلوماتية طريقة خاصة في التعامل مع المعلومة من خلال اسلوب الآلية، فإنه كان من الواجب و لأجل تحقيق ذلك و ضع نظم تحقق مفهوم الآلية ، و هي ما يعرف بالنظم المعلوماتية التي تكون في شكل آلات تعرف بإسم الحواسيب و شبكات الإتصال، كل ذلك لأجل تسريع و تسهيل نقل المعلومات و ضمان نقلها و سلامة أمنها ، بهدف ترقية عمل المؤسسات الحيوية للدولة و تيسير الحياة الشخصية لأفراد المجتمع من خلال وضعهم في حالة إتصال مباشر مع أجهزة الدولة من خلال النظم المعلوماتية المتوفرة فما هي ياترى طبيعة هذه النظم المعلوماتية من حيث مكوناتها المادية و المعنوية و التي تعتبر التجسيد العلمي و العملي لمفهوم المعلومات و المعلوماتية ؟

---

[1]- محمد علي العريان– مرجع سابق – ص 38.

[2]– تركي بن عبد الرحمان المويشير– مرجع سابق– ص 14.

الفرع الثاني : مفهوم النظم المعلوماتية – Systèmes informatiques

بإزدياد حجم المعلومات و كثافتها إزدادت الحاجة إلى تبادلها و نقلها من مكان إلى آخر، وهو ما أدى إلى إنتشار تقنية المعلوماتية، التي تهدف إلى معالجة المعلومات بصفة آلية بفضل التقنيات التي تتوفر عليها و التي هي نتاج تقاطع علوم الحاسوب و علم الإتصالات ، الأمر الذي ادى إلى إنتشارها بسرعة مذهلة عبر كافة أقطار العالم .[1]

إن النظم المعلوماتية هي عماد تقنية المعلوماتية فبدونها كان من المستحيل إحراز هذا التقدم على المستوى الحضاري، و قد يلتبس الكثير منا في محاولة وضع تعريف خاص بالنظم المعلوماتية نظرا لتشابه المصطلحات ، غير أننا سنحاول العمل على إبراز مفهوم النظم المعلوماتية و تعريفها بشكل يتوافق مع موضوعنا بعيدا عن التعقيدات التي تحملها التعاريف التي يقترحها علم النظم المعلوماتية.

الفقرة الأولى : تعريف النظم المعلوماتية .

تكفلت نصوص و احكام الإتفاقيات الدولية و الإقليمية إضافة إلى نصوص التشريعات الوطنية بتعريف النظم المعلوماتية ، فعرفت إتفاقية بودابست لمكافحة الجرائم المعلوماتية في مادتها الأولى النظم المعلوماتية بأنها " كل آلة بمفردها أو مع غيرها من الألآت المتصلة او المرتبطة ، و التي يمكن ان تقوم سواء بمفردها أو مع مجموعة عناصر أخرى تنفيذا لبرنامج معين بأداء معالجة آلية للبيانات المعلوماتية ، و تعني هذه الأخيرة كل تمثيل للوقائع أو المعلومات أو المفاهيم تحت أي شكل و تكون مهيأة للمعالجة الآلية بما في ذلك برنامج معد من ذات الطبيعة يجعل الحاسوب يؤدي المهمة".[2]

[1]– حسن طاهر داود – جرائم نظم المعلومات – الطبعة الأولى– جامعة نايف للعلوم الأمنية – الرياض– السعودية – 2000– ص 18.

[2] - إنبثقت إتفاقية بودابست عن إجتماع المجلس الأروبي و ذلك بتاريخ : 23 نوفمبر 2001 ، تحت رقم 185 و ذلك تحت وصف " إتفاقية بودابست لمكافحة الجريمة المعلوماتية" و هي إتفاقية تخص دول النطاق الأروبي و كذلك كافة دول العالم من خلال فتحها للتوقيع و التصديق من قبل باقي الدول خارج النطاق الأروبي، و هي الإتفاقية الموجهة لوضع الأطر القانونية لمكافحة الجرائم المعلوماتية ، و قد دخلت حيز التنفيذ بتاريخ : 01 جويلية 2004.

كما نجد تعريفا آخر جاءت به المذكرة التفسيرية لإتفاقية بودابست الصادرة قبلا و بتاريخ 2001/11/08 بمناسبة إنعقاد الدورة رقم 109 لإجتماع لجنة وزراء المجلس الأوربي ، بالقول بأنها " المقصود بالنظام المعلوماتي هو جهاز يتكون من مكونات مادية و مكونات منطقية ، بغرض المعالجة الآلية للبيانات الرقمية يشمل هذا الجهاز على وسائل الإدخال و إخراج و تخزين البيانات و قد يكون هذا الجهاز منفردا أو متصلا بمجموعة من الأجهزة المتماثلة عن طريق شبكة و تعني كلمة آلية دون تدخل بشري .[1]

أما على مستوى التشريعات الوطنية فقد عرفها نظام مكافحة الجرائم السعودي في مادته الأولى بأنها " مجموعة برامج و ادوات معدة لمعالجة البيانات و إدارتها و تشمل الحاسبات الآلية " ، أما المشرع الأردني فقد تولى أيضا إبداء تعريف صريح للنظم المعلوماتية بقوله بأن نظم معالجة المعلومات هي ذلك النظام الإلكتروني المستخدم لإنشاء رسائل المعلومات او إرسالها و تسلمها أو معالجتها او تخزينها أو تجهيزها على اي وجه آخر و ذلك وفق ما ورد في نص المادة الثانية 02 من قانون المعاملات الأردني رقم 85 لسنة 2001.

و هو الرأي الذي جاء به المشرع الجزائري بالقول بأن النظم المعلوماتية هي " أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها او أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".[2]

و بالعودة لمضمون التعاريف السابقة يمكن لنا أن نقترح تعريفا خاصا بالنظم المعلوماتية بالقول بأنها" **عبارة عن مجموعة من الحواسيب المنفردة او المتصلة ببعضها البعض بواسطة شبكات إتصال داخلية أو خارجية تعمل بصفة آلية وفق برامج مصممة خصيصا لأجل تحقيق معالجة آلية للمعلومات** "، و لذلك سنفصل شيأ ما في الفقرات اللآحقة مضمون هذه المفاهيم .

---

[1]– هلالي عبد اللاه أحمد – إتفاقية بودابست لمكافحة الجرائم المعلوماتية معلقا عليها – الطبعة الأولى– دار النهضة العربية – مصر – 2008– ص 19،18.

[2]– الفقرة "ب" من المادة 02 من القانون 04–09 المتعلق بآليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها

الفقرة الثانية: المكونات المادية للنظم المعلوماتية.

تعد الحواسيب (Ordinateurs ou computers)، من أهم المكونات الرئيسية للنظام المعلوماتي ، فما هي يا ترى أهمية هذا الجهاز في تكوين النظام المعلوماتي ؟

اولا :التعريف الإصطلاحي للحاسوب: يعرف الحاسب الآلي بانه " آلة تقوم بأداء العمليات الحسابية و إتخاذ القرارات المنطقية على البيانات الرقمية بوسائل إلكترونية و ذلك تحت تحكم البرامج المخزنة فيه ".[1]

كما يعرف بأنه " عبارة عن جهاز إلكتروني يتكون من عنصرين مادي و معنوي ، يشمل الأول كل المكونات المادية في حين يشمل الثاني البرامج حيث يتم تشغيله على ضوء برنامج يتم تخزينه على ذاكرته و من ثم يقوم بإستقبال البيانات و معالجتها على النحو المطلوب منه بغية الوصول إلى نتائج محددة".[2]

ثانيا : التعريف الفقهي للحاسوب : أما من ناحية الفقه فقد عرفه الفقه المصري بأنه " جهاز الكتروني يستطيع أن يقوم بأدق العمليات الحسابية و المنطقية للتعليمات المعطاة له بسرعة كبيرة قد تصل إلى عشرات الملايين من العمليات الحسابية في الثانية الواحدة ، و ذلك على درجة عالية من الدقة ، له القدرة على التعامل مع كم هائل من البيانات و كذلك تحزينها و إسترجاعها عند الحاجة إليها ".[3]

ثالثا : التعريف القانوني للحاسوب : للحاسوب نصيب من التعاريف القانونية فقد عرفه المشرع السعودي في نص المادة الأولى (01) من نظام مكافحة الجرائم المعلوماتية السعودي بأنه " أي جهاز إلكتروني ثابث أو منقول سلكي أو لا سلكي ، يحتوي على نظام معالجة البيانات أو تخزينها أو إرسالها أو إستقبالها أو تصفحها يؤدي وظائف محددة بحسب البرامج و الأوامر المعطاة له " .

[1]– خالد عياد الحلبي – إجراءات التحري و التحقيق في جرائم الحاسوب و الأنترنت– الطبعة الأولى – دار الثقافة للنشر و التوزيع – عمان– الأردن– 2011– ص 39.

[2]– محمد حماد الهيتي– التكنولوجيا الحديثة و القانون الجنائي– الطبعة الثانية– دار الثقافة للنشر و التوزيع–عمان– الأردن– 2012– ص 144.

[3]- محمد علي العريان– مرجع سابق – ص 56.

أما من ناحية التشريع الجزائري فنجد ان القانون 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها ، لم يتطرق لتعريف جهاز الحاسوب بالرغم من انه يعتبر الوسيلة و القطعة الأساسية لأي نظام معلوماتي .

إذن فالحاسوب و في مجال النظم المعلوماتية يعتبر الدعامة الأساسية و للتعامل مع المعلومات و ذلك نظرا للسرعة و القدرة الهائلة التي يتمتع بها في هذا المجال، و ذلك لتوفره على خصائص مادية و اخرى منطقية تجعل منه فريدا من نوعه في هذا المجال فما هي ياترى المكونات الداخلية المادية منها و المنطقية التي تمنحه هذا التميز عن غيره في مجال التعامل مع المعلومات .

رابعا : المكونات المادية للحاسوب .(Hard Ware): يقصد بالمكونات المادية للحاسوب الهيكل المادي المكون لنظام الحاسوب و يتكون أساسا من الوحدات الرئيسية التالية :

1-وحدات الإدخال: تستعمل هذه الوحدات لإدخال المعلومات أو الأوامر أو المعطيات أو البرامج المراد معالجتها إلى ذاكرة الحاسوب، و قد تكون في شكل و سائل إدخال مباشرة On Line، و تمثل لوحة المفاتيح keyborad إحدى هذه الوسائل،كما قد تكون في شكل وسيلة إدخال غير مباشرة Off Line، و كغرفة الأقراص المدمجة ، الماسح الضوئي.[1]

2-وحدة المعالجة المركزية Central Processing Unit C.P.U: و تعتبر مركز الأنشطة في الحاسوب وتحتوي على دوائر كهربائية تترجم و تنفذ تعليمات برامج التشغيل[2].

3-**وحدة الذاكرة Memory Unit M .U:** هي الوحدة التي تتم فيها عمليات تخزين المعلومات الواردة للجهاز أو النتائج الآتية من وحدة المعالجة المركزية .[3]

---

[1]- نهلا عبد القادر المومني-الجرائم المعلوماتية- الطبعة الثانية- دار الثقافة للنشر و التوزيع- عمان- الأردن- 2010- ص 24.

[2]- إبراهيم بن سطم بن خلف العنزي – التوقيع الإلكتروني و حمايته الجنائية – رسالة مقدمة لأجل نيل شهادة الدكتوراه- قسم العلوم الشرطية – جامعة نايف للعلوم الأمنية – الرياض – السعودية- 2009- ص 31.

[3] - المرجع السابق – ص 26.

4–وحدات الإخراج : و هي الأجزاء و الوحدات التي يتم من خلالها إخراج البيانات المعالجة من وحدة المعالجة المركزية غلى الخارج و من اهم وحدات اخراج الشاشة و الطابعة .[1]

خامسا: المكونات المنطقية للحاسوب (Software): تتمثل هده المكونات المنطقية في التطبيقات العملية التي تجري داخل الكيان المادي للحاسوب و تتمثل في جملة البيانات و المعلومات ، إضافة إلى برمجيات الحاسوب ولقد عرف القانون الأمريكي الصادر سنة 1988 الخاص بحماية حق المؤلف البرنامج Software ، بأنها مجموعة من التوجيهات او التعليمات التي يمكن للحاسب إستخدامها بشكل مباشر أو غير مباشر للوصول إلى تنيجة معينة ، كما يعرفها العاملون في مجال الحاسوب بأنها " الأوامر المرتبطة منطقيا و الموجهة إلى الحاسوب بعد توجيهها إلى اللغة الوحيدة التي يفهمها و هي لغة الأرقام الثنائية .[2]

الفقرة الثالثة : شبكات الإتصال كعنصر للنظم المعلوماتية .

يتكون النظام المعلوماتي من جملة من المكونات منها المتعلقة بالحاسوب من ماديات و برمجيات ، و منها ما يتعلق بالشبكات أي شبكات الإتصال ، و عليه فإن الجريمة المعلوماتية غالبا ما تنصب على إستغلال هذه المكونات من حواسيب و شبكات إتصال بإعتبارها القناة الرئيسية للوصول إلى المعلومات المخزنة او المتداولة بهدف الإعتداء عليها ، فما هي طبيعة هذة الشبكات و مدى اهميتها في مجال النظم المعلوماتية و في نظر المجرم المعلوماتي؟

أولا : مفهوم شبكة الإتصال : لشبكة الإتصال في مجال النظم المعلوماتية تعريف خاص يقصد به " أداة ربط بين حاسوبين او اكثر و هذه الرابطة قد تكون أرضية بالأسلاك او الكابلات ، كما يمكن ان تكون لا سلكية ، او بالأشعة تحت الحمراء ، أو بالقمار الصناعية ، و الشبكة يمكن ان تكون مقتصرة جغرافيا على منطقة صغيرة

---

[1]- عبد العال الدريبي – مرجع سابق – ص 18.

[2]- عبد العال الدريبي–مرجع السابق – ص 27.

فتسمى شبكة محلية Réseau Local ، كما يمكن ان تغطي منطقة كبيرة فتكون متسعة النطاق Réseau Etendu ، و يمكن ان تكون متصلة ببعضها البعض Interconnecté، و تعد شبكة الأنترنت internet، شبكة عالمية لأنها تتكون من العديد من الشبكات المتصلة ببعضها البعض و التي تستخدم جميعا نفس البروتوكولات ، والنظم المعلواتية يمكن ان تتصل بالشبكة بوصفها نقاطا نهائية او نقاط خروج ، أو كوسيلة لتسهيل نقل المعلومات .[1]

ثانــيا : تعريف شبكة الأنترنت : يعتبر الأنترنت أكبر شبكة حواسيب موسعة تغطي جميع انحاء العالم [2]، تتصل بين حواسيب شخصية و شبكات محلية و اخرى عامة ، يمكن لأي شخص حول العالم أن يصبح عضوا في هذه الشبكة من منزله او مكتبه او من اي مكان آخر بشكل يمكنه من الوصول إلى قدر هائل من المعلومات، و يكفيه لذلك حاسوب مكتبي او محمول و تقنية المودم.[3]

---

[1]– هلالي عبد اللاه أحمد– مرجع سابق – ص 23.

[2]- ظهر اول تصور نظري مكتوب لفكرة تواصل الحواسيب عن طريق شبكة في شهر أوت من سنة 1962 في مذكرات كتبها رئيس مركز أبحاث الكمبيوتر السيد" ليك ليدر–Licklider" ، و قد جرى أول إتصال بين حاسبين في مدينتين مختلفتين عام 1965 عن طريق خط الهاتف و كان احد الحاسوبين من نوع TX2، و الأخر من نوع Q–32 و لقد كان كل الفضل لوكالة الأبحاث التابعة لوزارة الدفاع الأمريكية تحت إسم " وكالة مشروعات الأبحاث المتقدمة " بتاريخ 21 نوفمبر 1969 و على يد "مات راكون" Racoon Matte في إنشاء أول شبكة حواسيب في الولايات المتحدة الأمريكية ، تحت إسم (ARPAnet) كإختصار لعبارة " شبكة وكالة مشروع الأبحاث المتقدمة" « Advanced Research Projects Agency Network »، إحتوت بدءاً على حاسوب مضيف واحد و مجموعة وصلات لم تتعد الأربع و هي : جامعة كالفورنيا بلوس انجلس و معهد ستانفورد للأبحاث و جامعة يوتا ، و جامعة سانتا بربارا ، و قد تم عرضها اول مرة للجمهور سنة 1972 في مؤتمر إتصال الحواسيب ، لقد كانت بدايات إستعمال شبكة الإنترنت عسكرية بحتة ، غير انها تحولت للإستعمال السلمي منذ سنة 1983 و ذلك بعد ربطها بعديد الجامعات الأخرى مما أدى إلى إزدحامها ، و لذلك أستحدثت شبكة جديدة عسكرية تحت اسم (Mil Net) ، و ترك امر الأولى لغرض تسهيل تبادل المعلومات البحثية العلمية فقط على مستوى مناطق الولايات المتحدة الأمريكية ، و إستمر الحال على ذلك إلى غاية منتصف التسعينات أين ظهرت إستخدامات أخرى للشبكة منها الخاصة و التجارية مما ادى إلى تطورها خصوصا بعد ظهور اول مستعرض للشبكة العالمية سنة 1993 تحت إسم (Mosaic)، و كل ما تلاه بعد ذلك من إصدارات العملاق (Microsoft) ، أدى إلى تطور هذه الشبكة و إمتدادها عبر قارات العالم . أنظر في ذلك : علي بن عبد الله غسيري – الأثار الأمنية لأستخدام الشباب للأنترنت – الطبعة الأولى– جامعة نايف للعلوم الأمنية– الرياض – السعودية – 2004– ص 38.

2- نهلا عبد القادر المومني – مرجع سابق – ص 35.

فشبكة الأنترنت عبارة عن وسيط ناقل للمعلومات بين اجهزة الحاسوب المتصلة به ،بواسطة أنظمة التحكم في البيانات ، وبروتوكولات و عناوين خاصة TCP /IP، حيث يتصل مستخدموها عن طريق الخط الهاتفي المتصل بمحول الإشارات المودم Modem[1]، الذي يقوم بتحويل الإشارات الرقمية و نقل الرسالة بين المرسل و المرسل غليه مرورا بالخادم Server.[2]

إذن فشبكات الإتصال تعتبر عنصرا مهما في تكوين النظام المعلوماتي فلا جدوى من الحاسوب المنعزل عن الشبكة في مفهوم النظام المعلوماتي مادام عاجزا عن التواصل مع باقي الحواسيب الأخرى ، و غير قادر على إرسال أو إستقبال المعلومات ، خصوصا و أن العالم اليوم يتمتع بأكبر نظام معلوماتي توفره له شبكة الأنترنت ، هذه الأخيرة التي تقدم خدمات عديدة كتبادل المعلومات ،البريد الإلكتروني، التجارة الإلكترونية ، التعاقد عن بعد ...إلخ من خدمات أخرى أصبح الإنسان غير قادر على الإستغناء عنها نظرا لما تسهم به هذه الأخيرة من تذليل للصعوبات و العقبات، غير أنها أصبحت المنفذ المفضل لمجرمي المعلوماتية لأجل تحقيق أهدافهم الإجرامية ،نظرا لإتصالها بأغلب الأهداف الإجرامية ، و بالموزاة مع ذلك أصبحت تشكل مسرحا للجرائم تمارس فيه إجراءات ذات طبيعة قانونية تهدف إلى البحث و التحقيق في شأن هذه الجرائم بغرض الكشف عن ملابستها و القبض على مرتكبيها بفضل إجراءات مستحدثة لم تكن معروفة مسبقا.

إذن فالنظم المعلوماتية هي عصب حياة تكنولوجيا المعلوماتية من خلال ما توفره من وسائل و تقنيات عالية في مجال التعامل مع المعلومة بفضل الحواسيب و شبكات الإتصال، و قد خلفت هذه النظم بمزاياها اثارا إيجابية لا محالة لا يمكن حصرها ، فأصبحت الحكومات و الشعوب تعتمد على هذه التقنية بالكامل من اجل تعزيز قدراتها الأدائية، كما تعمل و بشكل دوري على تطويرها و زيادة فعاليتها و قدراتها، غير أن هذا التطور

---

[1]– لمزيد من التفصيل حول مفهوم – البروتوكول– عنوان Tcp /Ip – Server– Modem– يرجى الإطلاع على قاموس المصطلحات المعلوماتية الملحق بالبحث رقم : **01**

[2]– علي بن عبد الله غسيري – مرجع سابق– ص 13،14.

اللامتناهي لتقنية المعلوماتية و اثرها على نمط الحياة خلق نوعا من الشعور بالتهديد و اللأمن بسبب صور الإعتداءات الإلكترونية التي تستهدف هذه النظم المعلوماتية بما تختزنه من معلومات شخصية و مالية و سرية...إلخ ، و هو ما إستدعى ظهور فرع جديد من العلوم يعرف بمجال الأمن المعلوماتي.

الفرع الثـالث : الأمـن المعلوماتي .

إن تنامي إستعمالات تقنية المعلوماتية و ظهور مفاهيم جديدة ، كالحكومات و الإدارات والعقود الإلكترونية ، و إنتشار مواقع التواصل الإجتماعي على شبكة الأنترنت ، و إعتماد كل منا على هذه الوسائل في حياته اليومية ، يحمل نوعا من الخطر يتمثل في صور الإعتداء التي يمكن ان تمس بالمعطيات الرقمية لكل منا ، و ما يمكن ان تسببه من ضرر في صورة الاثار السلبية للجريمة المعلوماتية ، وهو ما ادى إلى ظهور و بشكل موازى لتقنية المعلوماتية ما يعرف بالأمن المعلوماتي ، فما هو يا ترى هذا المجال الأمني الحديث و ما هي ابعاده في مجال نظم المعلوماتية ؟

الفـقرة الأولى : تـعريف الأمن المعلوماتي .

يعرف الأمن المعلوماتي بأنه " فرض ضوابط على سبل و أساليب الوصول للمعلومات ،بهدف إضفاء الشرعية على حدود و صلاحية إستخدام المعلومات" ، كما عرف أيضا بأنه " إتخاذ الإحتياطات و التنظيمات التي تهدف إلى المحافظة على المعلومات في الحاسوب ، بمأمن من الأعطال و الحوادث او الجرائم المتعمدة".[1] و تهدف اغلب التعاريف إلى إبراز ان الأمن المعلوماتي ينطوي على :

- المحافظة على المكونات المادية للحاسوب.
- المحافظة على المعلومات و سلامتها و سريتها و ملكيتها و الإستفادة منها .

[1]– عبد الله بن سعود محمد السراني – مرجع سابق– ص 23.

- المحافظة على المعلومات من تداخل إستخدامها او تخريبها ، أو إستخدام معلومات مضللة ، أو تحريفها و إستبدالها ، او سوء تفسيرها و إلغائها أو الفشل في إستخدامها او سرقتها.
- معالجة جميع الخروقات المتعلقة بالسلامة و السرية ، والملكية لصاحب المعلومة .

و يمكن إيجاز كل ذلك في إطار تعريف موجز واحد مضمونه " الأمن المعلوماتي هو ذلك العلم الذي يبحث في إستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها و انشطة الإعتداء عليها ".[1]

و يتمتع مجال الأمن المعلوماتي بالأهمية البالغة نظرا لإزدياد أهمية و قيمة المعلومات، و دورها الحساس، بالنسبة للدول خصوصا تلك الأمنية و العسكرية و الإقتصادية ذات الطابع الإستراتيجي ، لذلك إرتبط عنصر السرية بالمعلومات على ضوء ما قد يترتب جراء فقدانها من خسائر .[2]

ضف إلى ذلك ان تقنية المعلوماتية قد خلفت و على صعيد الحياة الشخصية سلسلة من التحديات الجديدة ، و التهديدات الخاصة فهي تزيد من كمية البيانات المجمعة و المعالجة ، بإعتبارها مصدر غني بالمعلومات المتعلقة بالحياة الشخصية للأفراد ، فتوفر عنهم معلومات متعلقة بعاداتهم ، هوياتهم و سلوكياتهم ،و أرائهم و إتجاهاتهم ، و تتدفق هذه المعلومات عبر الحدود دون أي إعتبار للحدود الجغرافية و السياسية ، و قد تعرض لجهات داخلية و خارجية ، و ربما لجهات غير معروفة و هذا ما ينجر عنه إساءة إستخدامها في دول لا تتوفر فيها مستويات الحماية القانونية للمعلومات بشكل كاف.[3]

---

[1]– عمر بن محمد العتبي – الأمن المعلوماتي و مدى توافقه مع المعايير المحلية و الدولية – رسالة مقدمة لأجل نيل شهادة الدكتوراه – قسم العلوم الشرطية– جامعة نايف للعلوم الأمنية – الرياض – السعودية– 2010– ص 15.

[2]– عبد الله بن سعود محمد السراني – مرجع سابق– ص 24.

[3]– بولين أنطونيوس أيوب – الحماية القانونية للحياة الشخصية في مجال المعلوماتية – دراسة مقارنة – الطبعة الأولى– منشورات الحلبي الحقوقية– بيروت – لبنان– 2009– ص 21.

الفقرة الثانـية : غايات الأمن المعلوماتي .

تتمثل الغايات الأساسية لإعتماد إستراتيجيات الأمن المعلوماتي في أي منظومة معلوماتية ، في الحفاظ على المعلومة من حيث :

أولا : الإتاحة: أي إتاحة إستخدامها بصورها الأصلية أينما كانت و كيفما تطلب الأمر ، أي حفظ المعلومات من مظاهر التخريب أو الخلط مع معلومة اخرى على نحو يلوثها .

ثانيا : التكامل: يقصد بالتكامل هنا تكامل المحتوى أي ان المعلومات المعالجة آليا كل لا يتجزأ، و الأمن المعلوماتي هو ما يضمن سلامة المعلومة بكل أجزائها منذ بدء المعالجة و إلى نهايتها ، من خلال ضمان عدم التلاعب بالمعلومات سواء بشكل جزئي أو كلي.[1]

ثالـثا : السـرية : اي ضمان حفظ المعلومات المخزنة او المنقولة عبر الشبكة و عدم الإطلاع عليها أو إستخدامها إلا بموجب إذن ، أي ضمان الإطلاع عليها لفائدة المصرح لهم ، فضلا عن تحديد حدود صلاحية الإستخدام كلية كانت او جزئية ، سواء ما تعلق منها بالحق في القراءة فقط او بالحق في الحذف و التعديل.[2]

مما سبق يتضح لنا ان النظم المعلوماتية و في ظل الحاجة المتزايدة عليها، تتطلب زيادة في الحاجة إلى إستراتيجيات و تقنيات الأمن المعلوماتي، و ذلك نتيجة لتزايد مظاهر الإجرام المعلوماتي ، من خلال إنتشار هذه التقنية و طغيان مظاهر إستعمالاتها اليومية على حياتنا ، فاي تهاون او فراغ في هذا المجال سيشكل و بدون شك منفذا لمحترفي الإجرام المعلوماتي مما يشكل تهديدا على المصالح الأساسية للدولة و خصوصا منها الدفاعية العسكرية و المالية و الصحية ، إضافة للمصالح الشخصية للأفراد التي تتنامى يوما بعد يوم على مستوى المجال الرقمي ، خصوصا و ان التكنولوجيا المعلوماتية أضحت مكتسبة في شكل هاتف نقال ذكي ، تصول و تجول أينما حل حامله و لذلك إهتمت التشريعات و على إختلاف قناعاتها بمفهوم الجريمة المعلوماتية

[1]– سلمى مانع – دور الأمن المعلوماتي في مكافحة الجرائم المعلوماتية– بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة- 16و 17 نوفمبر 2015- كلية الحقوق – جامعة بسكرة- الجزائر ص 10.

[2]– عبد الله بن سعود محمد السراني – مرجع سابق– ص 25.

ووضعت إستراتتيجيات امنية حديثة بهدف محاربتها و مجابهة مجرميها الذين يتمتعون بميزات و خصائص فريدة من نوعها تجعل من امر ملاحقتهم و عقابهم امرا صعبا بالنظر إلى خصوصيات جرائمهم و الأساليب التي يتسترون خلفها و هي المسائل التي سنحاول ان نعالجها في إطار نظري في المطلب الموالي.

المطلب الثاني:الجريمة المعلوماتية.

إن التطور التكنولوجي و ما صحبه من ثورة في مجال المعلوماتية الناتجة عن الاستخدام المتزايد لأجهزة الحاسوب بمختلف أشكاله وأنواعه، المكتبية، المحمولة، الهواتف الذكية والمتصلة على شبه الدوام بشبكة الأنترنت، أثر وبشكل على مظاهر حياة الأفراد والمجتمعات بشكل إيجابي، من خلال مختلف الصيغ الإلكترونية المتاحة والتي تجعل من أمر قضاء الفرد لمختلف حاجياته (التعلم، الصحة، التواصل، إبرام العقود، طلب الوثائق، الإدارية....إلخ) ، مجرد أمر بسيط لا يقتضي منه سوى الكبس على زر أو ملامسة شاشة رقمية، بدل التنقل من مكان لآخر، وهو عكس ما كان عليه الحال سابقا، غير أن مظاهر التمدن التكنولوجي هذه، صاحبتها ظواهر سلبية عدة بظهور الجريمة المعلوماتية التي استقطبت فئة جديدة من المجرمين اتخذوا من هذه التقنية (نظم المعلومات) أداة للإجرام في في شكل معاصر،بشكل قلب مفهوم الإجرام التقليدي من خلال وتيرتها المتسارعة من حيث سرعة تطورها والمجالات التي ستستهدفها وأثارها، و هو ما دفع بالباحثين في شتى المجالات سواء منها المعلوماتية التقنية، الاجتماعية، والقانونية خصوصا إلى مباشرة أبحاث معاصرة من أجل تحديد مدلول هذه الجريمة وذلك كل حسب مجال اختصاصه، وذلك من خلال تشريحها لأجل معرفة دوافعها ووضع حلول جدية في مواجهتها، وهي الإشكالات التي سنتناولها في هذا المطلب، ولكن قبل الولوج إلى مختلف المفاهيم الدالة على موضوع الجريمة المعلوماتية كان من الواجب علينا التطرق إلى تاريخ هذه الجريمة (الفرع الأول)، ثم بيان مفهومها (الفرع الثاني) وأخيرا تحديد خصائصها (الفرع الثالث).

الفرع الأول: التطور التاريخي للجريمة المعلوماتية.

إن التعرض لمفهوم الجريمة المعلوماتية يستلزم منا بالضرورة، التعرض لأهم المحطات التاريخية التي كانت ولا زالت تعتبر نقاط تحول في مسار السلوك الإجرامي التقليدي،إلى ذلك السلوك الإجرامي المعاصر والمعلوماتي.

و إذا أردنا الحديث عن الجريمة المعلوماتية باعتبارها ذلك النشاط الناشئ عن الإستغلال غير المشروع للحواسيب والشبكات المتصلة بها فيجب علينا الرجوع إلى المحطات التاريخية التالية:

- سنة 1981 أين تم تقديم (إيان مريفي–IAN MURPHY) أمم الجهات القضائية الأمريكية بتهمة الولوج غير المشروع للنظام المعلوماتي لشركة (AT&T) و تعمده تغير النظام الفوترة المعمول به.
- سنة 1986– تاريخ ظهور أول فيروس معلوماتي تحت اسم (Brain) والذي يهاجم حواسيب علامة IBM، وكان ذلك بالباكستان، وهي نفس السنة التي شهدت استصدار الكونغرس الأمريكي لأول قانون يجرم مسائل الغش المعلوماتي .
- سنة 1988 إطلاق (روبير موريس– ROBERT MORIS) لأول فيروس على شبكة الأنترنت عرف باسم" دودة موريس" والتي تسببت في إتلاف 6000 حاسوب كان متصلا بالشبكة وقد عوقب إثر ذلك بالحبس لمدة 03 ثلاث أشهر وبغرامة 10.000 دولار أمريكي.
- سنة 1990 إنتشار أكثر من 1000 نوع من الفيروسات على شبكة الأنترنت .
- سنة 1994 قيام عالم الرياضيات الروسي (فلاديمير ليفين–VLADIMIRE LEVIN) بالإستيلاء إلكترونيا على مصرف (City bank) من خلال الدخول إلى النظام المعلوماتي المصرفي العالمي (SWIFT)، وهو ما حقق له ثروة قدرت بـ 10 ملايين دولار أمريكي، وتسبب في خسارة هذا البنك لأكبر 10 زبائن له، وقد ألقي عليه القبض بلندن سنة 1995 وتم تسليمه للولايات المتحدة الأمريكية، التي أصدرت في حقه بالسجن لـ 03 ثلاث سنوات.لتتوالى في حقبة التسعينات الجرائم

المعلوماتية سواء تلك الناتجة عن نشر الفيروسات أو تلك المتعلقة بالتعدي على الأموال ولعل أن أهم هذه الحقبة هو حكم الإعدام الذي صدر في حق مواطنين صنيين أتهما باختراق نظام المعلومات الخاص بأحد البنوك الصينية وتحويل ما قيمته 87000 دولار أمريكي لحسابهما الشخصي.

لتأتي بعد ذلك حقبة سنوات الألفين (2000) والتي تميزت بظهور أنواع أخرى وحديثة من مظاهر الإجرام المعلوماتي، تتسم بالخطورة على أمن الفرد والجماعة، من خلال استهدافها لشتى المجالات،سواء منها الحيوية للدولة أو الأفراد فأصبحت الجريمة المعلوماتية سلوكا نتعايش معه يوميا في ظل التهديدات التي تشكلها على مصالحنا الخاصة والعامة ، ونظرا لاعتمادنا المتزايد يوما بعد يوم على تقنية المعلوماتية.[1]

إن هذه المظاهر السلبية الناتجة عن الإستخدام غير المشروع لتقنية المعلوماتية دفعت بأغلب الحكومات إلى وضع تشريعات وقائية منها وعقابية لأجل مواجهة هذه الظاهرة الإجرامية، وقد شكل موضوع تعريفها وتحديد مدلولها حاجزا حقيقيا في إطار توحيد الجهود لمحاربتها على نطاق دولي، ولذلك سنحاول جاهدين معالجة موضوع تعريف الجريمة المعلوماتية في الفرع الموالي.

الفرع الثاني: تعريف الجريمة المعلوماتية.

إستقطب مفهوم الجريمة المعلوماتية اهتمام الفقهاء والقانونيين والمختصين في مجال المعلوماتية، من أجل وضع تعريف شامل للجريمة المعلوماتية، فحاول كل منهم حسب اختصاصه وضع تعريف ملائم فمنهم من عرفها تعريفا ضيقا وقال بأنها " الجرائم المرتبطة بالحاسوب والتي تشكل انتهاكا للقانون الجنائي" ومنهم من قال بأنها " تلك الجريمة التي يستخدم فيها الحاسوب" وهو تعريف واسع جدا.[2]

[1] Jean- Philippe Humbert- le monde de la cyberdélinquance et l'image sociale du pirate informatique - thèse de doctorat- sciences de l'information est de la télécommunication - université Paul Verlaine –Metz – France – 2007- P 95-97.

[2] – عمر بن محمد العتبي – مرجع سابق – ص 21.

و إذا ما حاولنا وضع تعريف متكامل لهذا النوع من السلوك الإجرامي، فإنه يجب علينا الإطلاع بدءا على مدلولها باللغة الفرنسة (La Cybercriminalité) فأصل الكلمة (Cyber) يوناني (Kubernan)أي التحكم والتسيير، ويقصد به في مجال المعلوماتية المعالجة الآلية للمعطيات ، وقد شاع استعمال هذا المصطلح واتصل بكافة صور الإجرام كالغش المعلوماتي (Cyber fraude) الإرهاب المعلوماتي (Cyber terrorisme).[1]

أما من الناحية القانونية فلا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن سوء استغلال النظم المعلوماتية أو إساءة استخدامها فهناك من يطلق عليها وصف جريمة الغش المعلوماتي، وهناك من يطلق عليها وصف جريمة الاختلاس المعلوماتي، وهناك من يصفها بجرائم الاحتيال المعلوماتي، غير أن المصطلح الأكثر شيوعا هو مصطلح الجريمة المعلوماتية.[2]

وقد تعددت التعارف الواردة بشأن الجريمة المعلوماتية بتعدد النظم والتشريعات والاتجاهات الفقهية فعرفت بأنها:

الفقرة الأولى: التعريف الإصطلاحي.

عرفت منظمة التعاون الاقتصادي والتنمية سنة 1983 (O.E.C.D) الجريمة المعلوماتية بأنها " كل وفعل وعمل غير مشروع، أو مخالف للأنظمة وغير مرخص، يستهدف أنظمة المعالجة الآلية للمعلومات أوتبادلها أو نقلها" وتشمل الجريمة المعلوماتية بهذا المفهوم " كل الجرائم التي يمكن أن تقع أو تمس بشبكات الاتصال بصفة عامة، وشبكة الأنترنت بصفة خاصة.[3]

وقد ورد تعريف الجريمة المعلوماتية بحسب ما قدمه مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين الذي عقد "بفينا" سنة 2000 بأنها " كل جريمة يمكن ارتكابها بواسطة نظام حاسوبي أوشبكة حاسوبية

[1] Myriam Quéméner- Yves Charpenel – La Cybercriminalité- Edition Economica- Paris- France-2010-p 07

[2]– تركي بن عبد الرحمان المويشير – مرجع سابق – ص 15.

[3] Myriam Quéméner- Yves Charpenel - La Cybercriminalité - op.cit.p 08.

أو داخل نظام الحاسوب وتشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية، ومن التعاريف الذي تم التوسع فيها تعريف الخبير الأمريكي (باركر- Parker) الذي حاول إعطائها مفهوما واسعا يحيط بكل أشكال التعسف في مجال استخدام النظم المعلوماتية ، فهي من وجهة نظره " كل فعل إجرامي متعمد أي كانت صلته بالمعلوماتية ينشأ خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل".[1]

إذن فما يمكن استنتاجه من جملة هذه التعاريف أن الجريمة المعلوماتية هي تلك الجريمة المرتبطة أساسا، بمظاهر التقدم التكنولوجي وهو ما يفسر اتجاه البعض لإطلاق مصطلح" جرائم التقنية الحديثة" على هذا النوع من الجرائم التي رشحها علماء الإجرام للتطور مستقبلا بالنظر إلى التقنيات الحديثة التي تظهر يوميا وبشكل دائم ومستمر.

الفقرة الثانية: التعريف الفقهي.

في إطار مساهمة الفقه في تعريف الجريمة المعلوماتية إنقسم هذا الأخير إلى إتجاهين أساسيين أحدهما اعتمد التضيق والآخر التوسع في إطار وضع تعريف الجريمة المعلوماتية.

-**أولا : الاتجاه الفقهي الذي يعرفها بشكل ضيق** : تزعم هذا الاتجاه الفقيه (ميروي- Merwe) من خلال وضعه تعريفا مضمونة " أن الجريمة المعلوماتية هي ذلك الفعل غير المشروع الذي يتورط في ارتكابه الحاسب"[2]، كما عرفها (روزبلات- Rosblat) بأنها "نشاط غير مشروع موجة لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي تحول عن طريقه" أما (سولريز-Solerez) فعرفها بأنها" أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات".[3]

---

[1]- تركي بن عبد الرحمان المويشير – مرجع سابق – ص15، 16.

[2]- محمد أمين الشوابكة – جرائم الحاسوب و الأنترنت(الجريمة المعلوماتية)- دار الثقافة للنشر و التوزيع- عمان الأردن- 2009 – ص 08.

[3]- محمد سيد سلطان – قضايا قانونية في امن المعلومات و حماية البيئة الإلكترونية- دار ناشري للنشر الإلكتروني – الكويت- سنة 2012 – ص 62.

مرجع متوفر على الموقع الرسمي لدار ناشري للنشر الإلكتروني- تاريخ التصفح2015/02/05- الرابط الإلكتروني:
http://www.nashiri.net/latest/books-mags-news/5051-2012-01-27-22-05-28-v15-5051.html

الملاحظ أن هذه التعاريف تستند إلى موضوع الجريمة ونمط السلوك محل التجريم، دون أن تأخذ بعين الاعتبار المجرم وهو ما أدى ببعض من الفقهاء إلى وضع تعاريف أخرى ذات طابع موسع ، تستند إلى الفاعل بدل موضوع الجريمة.

-**ثانيا: الاتجاه الفقهي الموسع لمفهوم الجريمة المعلوماتية** : حاول هذا الاتجاه إعطاء تعريف موسع للجريمة المعلوماتية لهدف تفادي النقص الظاهر على التعاريف السابقة، فعرفت بأنها " كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع للتقنية المعلوماتية بهدف الاعتداء على الأموال المادية أو المعنوية" كما عرفت بأنها " كل سلوك سلبي كان أم إيجابي يتم بموجبه الاعتداء على البرامج أو المعلومات للاستفادة منها بأية صورة كانت".[1]

كما عرفت أيضا بأنها " كل عمل أو امتناع يأتيه الإنسان إضرارا بمكونات الحاسوب المادية والمعنوية وشبكات الاتصال الخاصة، باعتبار من المصالح والقيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها".[2]

وفي ذات الاتجاه يرى الفقيهان (ميشال وكريدو– Michel&Credo) أن سوء استخدام الحاسوب يشمل استخدام الحاسوب كأداة لارتكاب الجريمة، بإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسوب المجني عليه أو بياناته ، كما تمتد هده الجريمة لتشمل الاعتداءات المادية الماسة بالحاسوب ذاته،أو المعدات المتصلة به ، و كذلك الإستخدام غير المشروع لبطاقات الائتمان ، وتزييف المكونات المادية والمعنوية للحاسوب بل وسرقة جهاز الحاسوب في حد ذاته أو مكون من مكوناته.[3]

---

[1]– تركي بن عبد الرحمان المويشير– مرجع سابق– ص 17.

[2]– محمد أمين الشوابكة – مرجع سابق – ص 09.

[3]– محمد علي العريان – مرجع سابق – ص 45.

الفقرة الثالثة: التعريف القانوني.

عرف المشرع الجزائري الجريمة المعلوماتية في نص المادة 02- الفقرة -أ- من القانون رقم 09-04 المؤرخ في 05 أوت 2009 والمتضمن لقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات لإعلام والاتصال ومكافحتها بالقول بأن " الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي : جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية"

إذن وعملا بالتعاريف المقترحة للجريمة المعلوماتية ، فإنه يمكننا إقتراح تعريف خاص يشمل كافة الجوانب المتعلقة بالجريمة هذه فنعرفها بأنها " **كل السلوكات المجرمة التي يشكل الحاسوب وشبكات الاتصال الخاصة به وسيلة لارتكابها أو محلا لوقوعها، أي الجرائم التي ترتكب في البيئة الرقمية الإلكترونية.**

الفرع الثالث: خصائص الجريمة المعلوماتية.

إن مفهوم الجريمة المعلوماتية كما سبق والتطرق إليه، والقاضي بأنها ذلك النشاط الإجرامي المتصل باستعمال تقنية الحاسوب وشبكات الاتصال، يجعل من هذه الجرائم ذات طبيعة خاصة تختلف والمفهوم التقليدي المرتبط بتجريم السلوكات ذات الطبيعة المادية، والتي تترك أثرا ملموسا في العالم الخارجي ، ذلك لأن هذا النوع من الجرائم يتخذ من العالم الافتراضي ملجأ له بحيث لا تكاد تظهر السلوكات الإجرامية، نظرا لما تتميزبه هذه الجرائم من خصوصيات تجعل من أمر اكتشافها أمرا غاية في الصعوبة، وهي الإشكاليات والمسائل التي سنحاول جاهدين معالجتها في هذا الفرع الذي يحركه تساؤل أساسي متمثل في محاولة معرفة أهم الخصائص ومميزات الجرائم المعلوماتية ومقارنتها بمفاهيم الإجرام التقليدي.

الفقرة الأولى: الجريمة المعلوماتية عابرة للدول.

إن ارتباط كل دول العالم بشكة الاتصالات الدولية، من خلال الأقمار الصناعية، وشبكة الأنترنت جعل أمر عولمة الجريمة أمرا ممكنا وشائعا فأصبحت الجريمة لا تعترف بمفهوم الحدود الإقليمية للدول و اكتسحت الساحة العالمية.[1]

فأصبح من الممكن أن يرتكب الجاني جريمة في دولة ويكون المجني عليه في دولة أخرى، وقد يترتب الضرر على أماكن متعددة في العالم بسبب الجريمة الواحدة.

إن هذه الطبيعة التي تتميز بها الجريمة المعلوماتية بكونها عابرة للحدود خلقت العديد من المشاكل، حول تحديد الدولة صاحبة الاختصاص القضائي لهذه الجريمة، وكذلك حول القانون الواجب التطبيق، إضافة إلى إشكاليات لتعلق بإجراءات الملاحقة والمتابعة القضائية".[2]

فالمجرمون المعلوماتيون أصبحوا يقصدون دولا تخلوا تشريعاتها من قوانين مكافحة الجريمة المعلوماتية، من أجل القيام بأفعالهم الإجرامية، بينما تستشعر أفعالهم في باقي أنحاء العالم و هو ما جعل من أمر التحقيق و متابعة هؤلاء أمرا بالغا في التعقيد.

و قد أثار التقرير السنوي لمنظمة الأمن المعلوماتي (Symantec) لسنة 2009 أن نسبة الزيادة في النشاط الإجرامي المعلوماتي على المستوى العالمي قد بلغت 71 % مقارنة بـ 2008، وذلك راجع خصوصا إلى انتشار تكنولوجيا التدفق السريع للانترنت والتي تبنتها كل من الدول البرازيل ، الهند، بولونيا، رومانيا، تركيا وعدم تأقلمها بعد مخاطرها.[3]

[1]- عبد العال الدريبي – مرجع سابق- ص 55.
[2]- تركي بن عبد الرحمان الموبشير- مرجع سابق – ص 19.
[3] -Myriam Quéméner – Yves Charpenel-La cybercriminalité - Op cit – p 14.

إن هذه الإشكاليات قد دفعت بدول العالم إلى الدعوة إلى تكثيف الجهود من اجل محاربة الجريمة المعلوماتية ،و لعل أن أهم اتفاقية مفتوحة للتوقيع في هذا المجال في اتفاقية مجلس دول أرويا المعروفة باتفاقية بودابست المؤرخة في 2001/11/23 و التي انضمت إليها خارج النطاق الأوربي الولايات المتحدة الأمريكية في 2006/09/22 نظرا لأهميتها في مجال مكافحة هذا النوع من الجرائم على المستوى الدولي، إضافة إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المنبثقة عن اجتماع مجلسي وزراء الداخلية والعدل العرب بالقاهرة بتاريخ 2010/12/21 والتي صادفت عليها الجرائم في نفس اليوم إيمانا منها بضرورة تكاثف الجهود على مستوى منطقة الدول العربية في مجال مكافحة الجريمة المعلوماتية ، خصوصا والتحولات التي تعرفها هذه الأخيرة في مجال استعمال التقنيات الحديثة في مجال الاتصالات والنظم المعلوماتية.[1]

الفقرة الثانية: صعوبة اكتشاف الجريمة المعلوماتية.

تتسم بالجرائم المعلوماتية بأنها خفية و مستترة في اغلبها ، لان الضحية لا يلحظها رغم انها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة ، كإرسال الفيروسات او التجسس على البيانات المخزنة و لعل ان ما يزيد من خصوصية صعوبة إكتشافها هي :[2]

---

[1] كان لتأثير قضية قرص (الإيدز) أثر بالغ في لفت انتباه العالم لمدى البعد الدولي لجرائم المعلوماتية وتتخلص وقائعها في الأحداث التي دارت سنة 1989 بحيث قام البريطاني (جوزيف بوب–Josephe Bobe) بتوزيع عدد كبير من نسخ أحد البرامج الذي يهدف في ظاهرة إلى إعطاء نصائح متعلقة بكيفية الوقاية من المرض، غير أن حقيقة البرنامج كانت فيروسا (حصان طراودة Cheval de troi) يعمل على تعطيل الحاسوب وتظهر على الشاشة رسالة يطلب فيها من الضحية إرسال مبلغ مالي على حساب جوزيف بوب من أجل أجل تمكنية من مضاد الفيروس، و قد ألقي عليه القبض في 1990/02/03 بولاية أوهايو الأمريكية وسلم للمملكة البريطانية وقد وجهت له 11 أحد عشرة تهمة إبتزاز وقعت أغلبها في دول متفرقة من العالم، غير أن محاكمته لم تبلغ مراحلها النهائية بسبب حالته العقلية، و أعتبرت القضية من أهم القضايا المعلوماتية التي أبرزت للعالم خطورة الجريمة المعلوماتية بما أنها كانت ثمرة أول جهد دولي في مجال محاربة المعلوماتية. أنظر في ذلك: نهلا عبد القادر المومني – مرجع سابق– ص 51–52.

[2]– عبد المؤمن بن صغير– الطبيعة الخاصة للجريمة المرتكبة عبر الأنترنت في التشريع الجزائري و المقارن– بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة- 16و 17 نوفمبر 2015- كلية الحقوق – جامعة بسكرة- الجزائر ص 8.

أولا: سرعة التنفيذ: لا يتطلب أمر تنفيذ الجريمة المعلوماتية أكثر من وقت الضغط على لوحة المفاتيح، وزر الفأرة أو ملامسة الشاشة الرقمية غير أن هذا لا يعني أنها لا تتطلب إعدادا مسبقا من خلال توفير المعدات اللازمة و البرامج الضرورية لذلك.

ثانيا: التنفيذ عن بعد: لا تتطلب الجرائم المعلوماتية في أغلبها وباستثناء جرائم سرقة معدات الحاسوب، وجود الفاعل في مكان الجريمة، فيمكن له إتيان جريمته وهو في مكان بعيد أو في دولة أخرى فكيفيه في ذلك دخول الشبكة و اعتراض تحويل الأموال، أو تخريب المعلومات، أو التعدي على الغير.

ثالثا: إخفاء معالم الجريمة :عادة ما تكتسي الجرائم المعلوماتية طابعا خفيا فلا يمكن ملاحظة أثارها إلا بعد التدقيق والتمعن من قبل أهل الاختصاص.[1]

ولعل أن عملية (Mariposa) المشتركة بين الشرطة الإسبانية ومعهد باندا للأمن المعلوماتي في 03 مارس2010، و التي أفضت إلى اكتشاف شبكة عالمية من الحواسيب بلغ عددها 13 عشرا مليون حاسوب موزعة على 190 دولة كانت خاضعة للتحكم من قبل مجموعة من المجرمين المعلوماتين السلوفينين، في شكل شبكة خاصة خفية تعرف بإسم (Botnet) ، وقد كانوا يستعملون برنامجا خفيا في شكل فيروس يعرف بأسم (BOT) يهدف إلى اعتراض أرقام البطاقات البنكية والأشخاص المرتبطين بالشبكة بما في ذلك عدد كبير من المؤسسات المالية والبنكية، وقد استولى هؤولاء على ما يقارب 800.000 معلومة بنكية خاصة بالأفراد وقدر عدد الشركات التي مسها الاختراق بأكثر من 50% من الشركات على المستوى العالمي وبلغت الخسائر ملايين الدولارات.[2]

الفقرة الثالثة: الجريمة المعلوماتية جريمة ناعمة (soft crime).تتطلب الجرائم التقليدية استخدام الأدوات والوسائل المادية، والعنف غالبا أما هو الحال في جرائم المخدرات و الإرهابية و السرقات و السطو المسلح، إلا

[1]– عبد العال الدريبي – مرجع سابق – ص 55.

[2] Myriam Quéméner – Yves Charpenel – La cybercriminalité– Op cit – p 10.

أن الجرائم المعلوماتية تمتاز بأنها جرائم ناعمة لا تتطلب العنف على الإطلاق، فنقل البيانات من حاسوب لآخر، وسرقة الأرصدة البنكية لا يتطلب تبادل إطلاق النار مع رجال الأمن.[1]

إن كل ما يحتاجه المجرم المعلوماتي هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة، و قد يحتاج كذلك إلى وجود شبكة المعلومات الدولية، إضافة إلى الإرادة في تحقيق الغرض الإجرامي وكل ذلك دون عنف.[2]

الفقرة الرابعة: صعوبة إثبات الجريمة المعلوماتية.

إن أمر اكتشاف الجريمة المعلوماتية، أمر ليس بالسهل كما بيناه سابقا، و كذلك الحال إذا ما تعلق الأمر بإثباتها في حال اكتشافها فهو أمر بالغ في التعقيد و الصعوبة.

إن الجريمة المعلوماتية تتخذ من بيئة الحاسوب و الأنترنت ملجاً لها ، فهي عبارة عن حزمة من البيانات و المعلومات في شكل نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي مما يجعل أمرطمس الدليل ومحوه كليا أمرا متاحا للمجرم المعلوماتي.[3]

ضف إلى ذلك أن وسائل البحث و التحقيق التقليدية، لا تفلح غالبا في إثبات هذه الجريمة نظرا لتخصصها بمسارح الجرائم التقليدية، التي تسمح لهيئات الاستدلال و التحقيق بالكشف عن الجريمة، وذلك عن طريق المعاينة و التحفظ على أثارها المادية، لكن فكرة مسرح الجريمة المعلوماتية بتضاؤل دوره في الإفصاح عن أدلة الجريمة و ذلك للأسباب التالية.[4]

- أن الجريمة المعلوماتية لا تترك أثرا علاوة على صعوبة الاحتفاظ بآثارها إن وجدت.

[1] عبد العال الدريبي– مرجع سابق– ص 57.
[2] –تركي بن عبد الرحمان المويشير – مرجع سابق – ص 24.
[3] – نهلا عبد القادر المومني – مرجع سابق – ص 56.
[4] – تركي بن عبد الرحمان المويشير – مرجع سابق – ص 23.

- أن الجريمة المعلوماتية تعتمد على قمة الذكاء في ارتكابها مما يجعل المحقق التقليدي لا يجيد التعامل معها نظرا لضعف التكوين في مجال المعلوماتية، أو النقص في تقنيات ووسائل التعامل مع النظم المعلوماتية.
- أن الوصول إلى الحقيقة بشأنها يستدعي الاستعانة بخبرة فئة عالية المستوى في المجال المعلوماتي و هو أمر قد يصعب تحققه نظرا لقلة عددهم و انشغالهم بالتحقيق في جرائم أخرى.[1]

الفرع الثالث: الطبيعة القانونية للجريمة المعلوماتية.

بالنظر إلى التعاريف التي وردت لمفهوم الجريمة المعلوماتية، و جملة الخصائص و السمات التي تميزها، فإنه و بدون شك ستتبادر إلى أذهاننا فكرة التساؤل حول الطبيعة القانونية للجريمة المعلوماتية، فهي في ظاهرها جريمة غير مادية، أي بدون أثر مادي ملموس، فمجالها البيئة الإلكترونية مما يجعلها مختلفة كليا عن الجرائم الأخرى التي يرى التشريع الجنائي أنها تهدد مصلحة الغير العامة و الخاصة ، و في هذا الصدد و بالنظر إلى تقاطع مفهوم الجريمة التقليدية و المعلوماتية بالمصالح المحمية قانونا فقد انقسم الفقه حول تكييف طبيعة هذه الجريمة بين الوصف الخاص و العام لها.

الفقرة الأولى: الاتجاه الفقهي الذي يرى بأن الجريمة المعلوماتية جريمة من نوع خاص.

يستند هذا الاتجاه على فكرة، أن مجال الحماية القانونية هو المعلومة في حد ذاتها باعتبارها السند الأساسي للنظم المعلوماتية، و انطلاقا من أن وصف "القيمة" يضفى على الأشياء المادية القابلة للإستحواذ دون تلك المعنوية التي لا يمكن الاستحواذ عليها، فإن مجال الحماية المقرر لها هو في ضوء حقوق الملكية الفكرية فقط، و لعل أن فكر هذا الاتجاه الفقهي يتعارض و المفاهيم الحديثة للقانون الجنائي الذي يقر بأحقية توفير الحماية القانونية للمعلومة باعتبارها تكتسب صفة المال و هو ما تبناه أنصار المذهب الثاني.[2]

---

[1]– عبد العال الدريبي – مرجع سابق – ص 57.

[2]– محمد علي العريان –مرجع سابق– ص 49.

الفقرة الثانية: الاتجاه الفقهي الذي يرى بأن الجريمة المعلوماتية جريمة مستحدثة.

يتخذ هذا الاتجاه موقفا صريحا مفاده أن الجريمة المعلوماتية و باعتبارها جريمة تستهدف المعلومات، و باعتبار هذه الأخيرة مجموعة مستحدثة من القيم باعتبارها قابلة للإستحواد عليها بعيدا عن دعامتها المادية، كما أنها قابلة للتقويم بحسب سعر السوق متى كانت غير محظورة تجاريا، و أنها نتاج مؤلفها وتجمع بينها علاقة، و هو الرأي الذي جاء به الأستاذ فيفانتي– vivanti بقوله أن " فكرة الشيء أو القيمة لها صورة معنوية و أن نوع الحق يمكن ان ينتمي إلى قيمة معنوية ذات طابع اقتصادي وأن تكون جديرة بحماية القانون، و متى كانت المعلومات و البرامج المعالجة آليا ذات قيمة اقتصادية فإنه يحب معاملتها معاملة المال."[1]

إذن فالبيانات و المعلومات الموجودة داخل ذاكرة الحاسوب تعتبر من الأموال و لها قيمة مادية، فهي قابلة للنقل من حاسوب لآخر أو لقرص مضغوط أو البريد إلكتروني فهي و بالتالي مال منقول و إذا ما نقلت من دون رضا صاحبها فيطبق عليها قانون العقوبات.

ولقد استقر الرأي الراجح من الفقه على أن البرامج و المعلومات تخضع لمبدأ الحماية الجنائية، و البرامج والمعلومات ملك لصاحبها، إن سرقة دعامتها من الغير هي سرقة للمعلومات في حد ذاتها لأنه لا يمكن الفصل بين الدعامة و المعلومة محل السرقة.[2]

ولقد أخذت أغلب التشريعات بهذا الموقف ووفرت للمعلومات في مواجهة الجريمة المعلوماتية ترسانة من القوانين المكملة لقانون العقوبات، و قانون حماية حق المؤلف ، وذلك بهدف وضع حد للاعتداءات المتكررة على صفة الأموال المنقولة المتداولة عبر النظم المعلوماتية، و لعل أن المشرع الجزائري قد واكب هذا التيار من خلال القوانين المتلاحقة في هذا المجال ، و لعل أن أهمها هو التعديل الذي مس قانون العقوبات الصادر بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتضمن إدراج نوع جديد من الجرائم تحت وصف

[1] - محمد علي العريان– مرجع سابق– ص51.
[2] - خالد عياد الحلبي- مرجع سابق- ص 57.

جرائم المساس بأنظمة المعالجة الآلية للمعطيات و التي تضمنتها المواد من 394 مكرر إلى 394 مكرر 07، و قد جاء التعديل ليكرس مفهوم حماية المال المنقول الذي جاء به قانون حماية الملكية الفكرية و حقوق المؤلف، الذي سبق سنه بتاريخ 19 جويلية 2003 تحت رقم 03-05، لتأتي من بعده مجموعة من القوانين من نفس السياق نذكر منها على سبيل المثال لا الحصر، التعديل الذي مس القانون المدني بموجب القانون رقم 05-10 المؤرخ في 30جوان 2005، و الذي نص على صور العقد الإلكتروني، وكذلك القانون المعدل و المتمم لقانون التأمينات الاجتماعية رقم 83- 11 المؤرخ في 02 جويلية 1983 وذلك تحت رقم 08-01 المؤرخ في 23 جانفي 2008 ، و الذي سن قواعد التعامل بالبطاقة الإلكترونية من قبل المؤمن له و مبادئ الفوترة الإلكترونية، ليجسد المشرع نيته في محاربة الجريمة المعلوماتية بصفة واضحة سنة 2009 بموجب صدور القانون المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها وذلك بتاريخ 05 أوت 2009 بموجب القانون رقم 09-04 وقد تولى بموجبه ملئ الفراغ القانوني الذي شاب القانون 04-05 المعدل و المتمم لقانون العقوبات، إضافة إلى بيان أهم الأطر الإجرائية الكفيلة بمتابعة الجناة وعقابهم في ظل الشرعية الإجرائية هؤلاء الجناة المعلوماتيين الذين يتمتعون بخصوصيات لا مثيل لها تجعل من أمر اقتفاء أثرهم أمرا بالغا الصعوبة بالنظر إلى مهاراتهم و درجة ذكائهم في هذا المجال، و في مجال الإفلات من العقاب، وهي الصفات و الخصائص التي ستكون محل دراستنا في المطلب الموالي.

المطلب الثالث: المجرم و الضحية في جرائم المعلوماتية.

يطلق وصف المجرم عادة على كل شخص يبادر بمحض إرادته إلى الاعتداء على جملة القواعد العامة ذات الطابع العقابي، المنظمة لسلوكات الأفراد و التي يكون الهدف منها حماية المصالح العامة و الخاصة على حد سواء، و لطالما شرعت قوانين و نظم لأجل مجابهة هذه السلوكات الإجرامية و متابعة مرتكبيها، وقل ما ظهرت إشكاليات مستعصية في مجال متابعة المجرمين، بالرغم من تعدد فئاتهم و اختلاف جرائمهم من حيث السلوك و النمط و النتيجة ، فكانت كل الجرائم تحمل طابع المادية ، و كان من السهل تصنيفها

و تصنيف فئات مرتكبيها، و معرفة دوافعهم و غاياتهم الإجرامية، بل اتخاذ تدابير وقائية في مواجهة خطورتهم الإجرامية، نظرا لتشابه جرائم الصنف الواحد، و كذلك توحد أصناف و طبائع المجرمين، و لكن و بظهور تقنية المعلوماتية ظهرت جرائم لم تكن متصورة قبلا واقعها مختلف تماما عن واقع الجرائم التقليدية، سواء من حيث طبيعتها أو من حيث صفات مرتكبيها أو وسائل ارتكابها، و حتى كذلك من حيث طبيعة ضحاياها، فتحولت جرائم الإحتيال إلى جرائم إحتيال الكتروني و جرائم السرقة إلى جرائم سرقة المعلومات، و جرائم السب و القذف و الاعتداء على الأشخاص إلى جرائم المساس بالبيانات الشخصية ... و الخ من صور إجرامية تعددت أوصافها في المجال الإلكتروني، إن كل هذه التطورات إن دلت على شيء فإنها تدل على تحول جذري في مجال الجريمة و المجرم و المفاهيم المتعلقة بعلم الإجرام خصوصا، و لذلك كان من الواجب التعرض إلى الصور الحديثة للمجرم المعلوماتي (الفرع الأول)، و دراسة وسائل إجرامه (الفرع الثاني)، و في الأخير إلقاء الضوء على الضحية في مجال المعلوماتية (الفرع الثالث) .

الفرع الأول : شخصية المجرم المعلوماتي.

يعد الأستاذ (باركر– Parker) واحدا من أهم الباحثين الذين اهتموا بموضوع الجريمة المعلوماتية عموما، و بالمجرم المعلوماتي خصوصا، من خلال البحوث التجريبية التي قام بها سنة 1976 بالولايات المتحدة الأمريكية، و قد وضع مجموعة من السمات التي تميز المجرم المعلوماتي، و التي يساعد التعرف عليها مواجهة هذا النمط الحديث من المجرمين، و يرى الأستاذ (باركر– Parker) أن المجرم المعلوماتي و إن كان يتميز ببعض السمات الخاصة إلا أنه في النهاية لا يخرج عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب عليه.[1]

الفقرة الأولى : المجرم المعلوماتي ذو طبع اجتماعي .

يتسم المجرم المعلوماتي في كونه في العادة كائنا ذو طبع اجتماعي يتميز بقدرته على التكيف في بيئته الإجتماعية، بل أن بعضهم يتمتع بثقة كبيرة في مجال عمله، فالمجرم المعلوماتي لا يضع نفسه في حالة عداء

[1] عبد العال الدريبي- مرجع سابق- ص 58.

مع المجتمع الذي يحيط به، فهو يتوافق و يتصالح معه، و تزداد خطورته الإجرامية كلما زاد تكيفه الاجتماعي مع توافر الميول الإجرامي لديه، فشعوره بأنه محل ثقة و أنه خارج إطار الشبهات يدفعه إلى التمادي في ارتكاب جرائمه و التي لا تكتشف عادة .[1]

و من توابع خصائصه الاجتماعية أنه شخص يشعر بالخوف الدائم من أمر كشف جرائمه و افتضاح أمره، بالرغم من أن هذا الشعور يخالج كافة المجرمين، إلا أنها تصاحب مجرمي المعلوماتية بصفة خاصة لما يترتب على كشف أمرهم من إرتباك مالي وفقد للمركز الوظيفي، ومرد هذا الخوف أيضا هو انتمائهم إلى فئة اجتماعية متميزة، من حيث التعلم والثقافة وطبيعة العمل.[2]

الفقرة الثانية: المجرم المعلوماتي ذكي ومحترف.

إذا كان مرتكبي الجرائم التقليدية ليس لمستواهم التعليمي و لا لدرجة ذكائهم دور كقاعدة في نمط جرائمهم ، فإن مجرمي المعلوماتية لا بد أن يكونوا من المختصين في مجال المعلوماتية و لهم دراية و خبرة في مجال التعامل معها و فك رموزها ، فلا يمكن أن يرتكب هذه الجرائم إلا من له مهارة و معرفة فنية في مجال المعلوماتية ، و لا يشترط المؤهل العلمي لذلك فيمكن ان يرتكبها شخص ليس له المؤهل العلمي و لكنه على درجة عالية من الذكاء .[3]

وتبين إحصائيات العديد القضايا أن عددا من المجرمين لا يرتكبون سوى جرائم المعلوماتية، إي أنهم محترفون في هذا النوع من الإجرام دون أن تكون لهم صلة بأي نوع من الجرائم التقليدية.[4]

إن المجرم المعلوماتي يمكن أن يكون تصورا كاملا لجريمته وذلك قبيل تنفيذها و ذلك حتى لا يتفاجأ بأمور غير متوقعة من شأنها إفشال مخططاته أو تسبب في الكشف عنها، فالجرائم التي يرتكبها تتطلب منه

[1] تركي بن عبد الرحمان المويشير- مرجع سابق-ص 28.

[2] –نهلا عبد القادر المومني – مرجع سابق– ص 80.

[3] –محمد حماد الهيتي – مرجع سابق – ص 163.

[4] –عبد العال الدريبي – مرجع سابق– ص 58.

مقدرة عقلية وذهنية عميقة في مجال المعلوماتية، فلا يلجأ إلى استخدام العنف بل يتبع أسلوب الهدوء لتحقيق أهدافه، و لذلك فإن الإجرام المعلوماتي هو إجرام الأذكياء فالمجرم المعلوماتي يسعى وبشغف إلى معرفة طرق جديدة لا يعرفها سواه سمح له بالاختراق الحواجز الأمنية في البيئة الإلكترونية لأجل نيل مبتغاه.[1]

الفقرة الثالثة: المجرم المعلوماتي يتميز بقوة التحمل والصبر.

يحتاج المجرم المعلوماتي إلى القدرة على التحمل و الصبر، فقد يستغرق أمراختراق الكتروني، أو تحويل أموال ساعات طوال أو أياما لأجل تجسيده، ولذلك فإن قوة التحمل و المثابرة من السمات التي تساعد المجرم، المعلوماتي على نيل مبتغاه و رفع و تنمية قدراته و مهاراته فتكرار المحاولات يستغرق وقتا طويلا يحتم عليه التمتع بالصبر.[2]

الفقرة الرابعة : المجرم المعلوماتي يتمتع بالسلطة.

يقصد بالسلطة في هذا المجال، جملة الحقوق و المزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته، فكثير منهم لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة، و تتمثل عادة في امتلاك شفرة الدخول إلى النظام المعلوماتي، و إجراء المعاملات، وقد تكون هذه السلطة أحيانا غير مشروعة في حال سرقة شفرة الدخول.[3]

وقد يستغل المجرم المعلوماتي المزايا التي توفرها تكنولوجيا المعلومات وسلطته عليها فيدون بيانات وهمية، وغير صحيحية و يطلب الحاسوب اعتمادها عند إجراء بعض العمليات و مثالها الموظف المشرف على الموظفين على مصالح المحاسبة و صرف الأجور الذي يمكن أن يدرج أسماء بعض الموظفين الوهميين ضمن قائمة الموظفين ثم يمرر عملية صرف الرواتب و يتولى إيداع رواتب الموظفين الوهميين في حسابه الخاص

---

[1]– نهلا عبد القادر المومني – مرجع سابق– ص 77،78.

[2]-عبد الله بن سعود بن محمد السراني – مرجع سابق – ص 36.

[3]-عبد العال الدريبي – مرجع سابق – ص 61،60.

و لذلك فإن المهتمين بمجال المعلوماتية عادة ما ينبهون أصحاب المؤسسات إلى أخذ الاحتياطات اللازمة عند اختيار المشرفين على هذه المصالح.[1]

إذا فما يمكن استخلاصه من جملة الخصائص و المميزات التي تميز المجرم المعلوماتي عن غيره من المجرمين، أن الإجرام المعلوماتي هو إجرام الذكاء و الأذكياء، فلا يحتاج إلى استخدام القوة و العنف، فالذكاء هو مفتاح المجرم المعلوماتي لإتمام فعله ويمكن إجمال عدد من القواسم المشتركة بين هؤلاء المجرمين في عدة صفات هي في شبه إجماع ما بين الكثير من الفقهاء و علماء الإجرام نذكر منها:

– أن سنهم و أعمارهم تكون محددة مابين 18 سنة و 45 سنة.

– المهارة و الإلمام الكامل، والقدرة الفنية والتقنية الهائلة في مجال نظم المعلومات.

– إنتمائهم إلى طبقة المتعلمين و المثقفين.

– الثقة الزائدة بالنفس و الإحساس بإمكانية إتمام جرائمهم دون افتضاح أمرهم.

– عدم إدراكهم بأن سلوكاتهم تستوجب العقاب بفعل إقرارهم الذاتي بمشروعية الفعل.[2]

و على ذكر" الذاتية " فإن دوافع ارتكاب الجريمة هي المعيار الأساسي في تصنيف المجرمين المعلوماتيين، فما هي يا ترى أصناف هؤولاء؟

الفرع الثاني: أصناف وفئات مجرمي المعلوماتية.

يصنف مجرمو المعلوماتية إلى عدة أصناف و ذلك حسب درجة الخطورة التي يتميزون بها أو يشكلونها في مواجهة أمن نظم المعلومات، وكذلك بالنظر إلى حجم رغباتهم و دوافعهم الإجرامية ما بين الفضول و المزاح وتحقيق الغاية الإجرامية و يمكننا تصنيفهم إلى ما يلي:

---

[1]- الهاشمي الكسراوي- "الجريمة المعلوماتية"- مقالة علمية - مجلة القضاء و التشريع- العدد 07 – السنة 48 - جويلية 2006 مركز الدراسات القانونية و القضائية- وزارة العدل و حقوق الإنسان- الجمهورية التونسية- ص 17.

[2] محمد علي قطب –" الجرائم المعلوماتية وطرق مواجهتها" - الجزء الأول- بحث منشور على الموقع الإلكتروني لمركز الإعلام الأمني- أكاديمية الشرطة البحرينية- مملكة البحرين- أفريل 2011-ص14 – تاريخ التصفح : 2014/06/05- الرابط الإلكتروني: http://www.policemc.gov.bh/reports/2011/April/1-4-2011/634372714052375622.pdf .

الفقرة الأولى: صغار مجرمي المعلوماتية أو العابثون.

هم فئة الشباب الذين انبهروا بالثورة المعلوماتية و الحواسيب ، و تتمثل أفعالهم في الإنتهاك غير المسموح به لذاكرات الحواسيب خصوصا ، لأجل الإطلاع على ما تحتويه من معلومات بدافع الفضول ، فهؤلاء الشباب لا يقدرون مطلقا النتائج المختملة التي يمكن ان تؤدي لها أفعالهم غير المشروعة ، فميولهم للمغامرة و التحدي و الرغبة في الإكتشاف ، هو ما يميزهم عن المجرمين المحترفين في مجال المعلوماتية.[1]

و قد تباينت الآراء حول تصنيف هؤلاء الشباب في طائفة المجرمين لأنهم ينطلقون من ميول المغامرة و التحدي و الرغبة في الاستكشاف وهم لا يدركون خطورة أفعالهم ، فنادى البعض بالقول بأن هذه الفئة لا تسبب ضرر للنظام المعلوماتي، بل يرجع لها الفضل في كشف الثغرات الأمنية في تقنية المعلومات و بالتالي فهي تخدم الأمن المعلوماتي.[2]

أما الاتجاه الآخر فيرى هذه الفئة تصنف ضمن مجرمي المعلومات مثل غيرهم من المجرمين لأن أفعالهم تعد خطيرة من الناحية العلمية بالنظر إلى تعديها حدود الحواجز الجغرافية، و في الحقيقة فإنه لا يجب التقليل من شأن هؤلاء فقد تتعدى بواعثهم الهواية و العبث لتتحول إلى مراحل متقدمة و هي مرحلة احتراف هذه الجرائم.[3]

الفقرة الثانية: قراصنة المعلوماتية.

يمثل القراصنة تهديدا جديا و فعليا على أمن المعلومات، فهم عادة ما يحترفون الجريمة المعلوماتية ويقصدون من ورائها إحداث الضرر بالمجني عليه، أو تحقيق الربح و الكسب من خلال التعدي على مواقع وبيانات و معلومات خاصة بالمؤسسات و الأفراد ، و يمكن التفرقة بين نوعين من القراصنة حسب درجة خطورتهم و إختلاف بواعثهم:

---

[1] سامي على حامد عياد– الجريمة المعلوماتية و إجرام الأنترنت– دار الفكر الجامعي – الإسكندرية – مصر – 2007– ص 63.

[2] - تركي بن عبد الرحمان المويشير – مرجع سابق- ص 30.

[3] نهلا عبد القادر المومني – مرجع سابق- ص 82.

-أولا : القراصنة الهواة (Hackers) : هم فئة من مجرمي المعلوماتية يمتلكون عادة وسائل تقنية متطورة أكثر من تلك التي يستعملها العابثون، تكون عادة في شكل حواسيب متطورة و متصلة بشبكة الأنترنت إضافة إلى برامج معلوماتية نادرة، يتكون مجتمعهم من مبرمجين معلوماتين أصحاب خبرة في مجال علم الحواسيب و الشبكات، يميزهم الذكاء الحاد، ويمضون نصف أوقاتهم أمام شاشات الحواسيب، فالقرصنة بالنسبة لهم هي حياة ثانية، تأخذ حيزا مهما من الحياة الأولى، هدفهم مهاجمة مواقع الشركات الكبيرة و المؤسسات الحكومية، ومواقع القواعد العسكرية، الهاكرز ليسوا دائما سيئ النية فهم يريدون و بكل بساطة أخذ العبرة بزيارة أماكن ممنوعة على الشبكة ولا يقومون عادة سوى بالإطلاع على المعلومات.[1]

إن هؤلاء المجرمين عادة ما يشغلون مناصب محل ثقة ولهم شهادات تعلمية ،ومن أمثلة ذلك الطالب الأمريكي (إيان ميرفي–Ian Murphy) الذي عمد سنة 1981 إلى اختراق الملفات المخزنة بحاسوب الحكومة الفيدرالية الأمريكية بهدف الإطلاع على المعلومات ذات الطابع السري فقط.[2]

و ما يمكن الإشارة إليه في هذا المقام هو التنظيم الذي أضحى يعمل عليه و يعتمده الهاكرز من خلال تبادل المعلومات والخبرات و الحلول، و تنظيم أنفسهم في مجموعات تعمل أو تدعي العمل للمصلحة العامة كمجموعة (Anonymosse) أو منظمات أخرى تعمل على تعطيل المواقع الإباحية و المواقع التي تنشر صور إباحية للأطفال، و الحقيقة التي يجب عدم إغفالها أن للقراصنة الهواة دورا يسهم في كشف الفجوات الأمنية، الأمر الذي يدفع إلى تطويرها ضد الإعتداءات.[3]

ثانيا: القراصنة المحترفون(Crackers) : يشكل الكراكرز أكبر تهديد للأنظمة المعلوماتية، لأنهم غير معروفين، ويستخدم هؤلاء عادة نفس وسائل القراصنة الهواة لدخول النظام المعلوماتي، لكنهم يختلفون معهم من

---

[1] بولين أنطونيوس أيوب - مرجع سابق- ص 185.
[2] الهاشمي الكسراوي – مرجع سابق- ص 185.
[3] نهلا عبد القادر المومني- مرجع سابق- ص 83،84.

حيث الباعث و الغاية، فهم لا يهدفون إلى سرقة المعلومات أو الإطلاع عليها فقط أو تعديلها، و إنما هدفهم هو تدميرها، ومسح النصوص و البرامج و المعلومات المسجلة على القرص الصلب للحاسوب.[1]

تعكس هذه الفئة ميولاتها الإجرامية الخطيرة التي تنبئ عن رغبتها في إحداث التخريب، فهم يتميزون بقدرتهم العالية و خبرتهم الواسعة في مجال النظم المعلوماتية، و عادة ما يعود المجرم المعلوماتي المحترف إلى ارتكاب جريمته مرة أخرى، بحيث تزداد سوابقه القضائية، و يعيش غالبا من عائدات جرائمه، وهذا المجرم لا يهتم بإبداء أراء متطرفة أو الدفاع عن حق الغير، وإنما يهتم فقط بالأفكار التي تدر عليه الأرباح.[2]

و تشير الأبحاث و الإحصائيات التي أجراها معهد (Stand Ford Resarch) أن الكراكرز هم من الجيل الحديث أي أنهم من فئة الشباب، وتتراوح أعمارهم ما بين 25-45 سنة وأن نسب ارتكابهم للجرائم مقسمة بـ:

- 25% من الجرائم المعلوماتية يرتكبها المحللون المعلوماتيون.
- 18% من الجرائم المعلوماتية يرتكبها المبرمجون المعلوماتيون.
- 17% من الجرائم المعلوماتية يرتكبها أشخاص لهم أفكار خاصة.
- 12% من الجرائم المعلوماتية يرتكبها أشخاص غرباء عن مكان تواجد المعلومات.
- 11% من الجرائم المعلوماتية يرتكبها فنيو التشغيل
- 17% من الجرائم المعلوماتية يرتكبها أشخاص من متصفحي الشبكات.[3]

إذا كان هذا التصنيف لمجرمي المعلوماتية هو التصنيف المتعارف عليه في ميدان الجرائم المعلوماتية فإنه هناك أنواع أخرى من مجرمي المعلوماتية يصنفون تصنيفا آخر يمكنهم ذكرهم على سبيل الحصر في فئة:

---

[1] بولين أنطونيوس أيوب - مرجع سابق- ص 186.

[2] نهلا عبد القادر المومني- مرجع سابق-ص 84.

[3] تركي بن عبد الرحمان المويشير- مرجع سابق- ص 32.

1. **الموظفون العاملون في مجال الأنظمة المعلوماتية:** يعتبر هؤلاء وبالنظر إلى المهارات التي يتمتعون بها، فئة مرشحة لأن ترتكب جرائم معلوماتية تحقق أهدافهم الشخصية وأهمها الكسب المادي أو الانتقام من أرباب العمل.

2. **مجرمو المعلوماتية المتطرفون:** ويتألفون عادة من أفراد الجماعات الإرهابية و المتطرفة في إطار الجريمة المنظمة، لهم من المعتقدات والأفكار الإجتماعية والسياسية والدينية، والتي يرغبون في فرضها باللجوء إلى النشاط الإجرامي الذي أصبح يتجه إلى الجرائم المعلوماتية.[1]

الفرع الثالث: الضحية في الجريمة المعلوماتية.

إن التسليم بأهمية النظم المعلوماتية و بالنجاح الكبير الذي حققته، لا يغفل معه أثر هذه النظم السلبي على ضمانات الحق في الحياة الخاصة، و يتجلى ذلك بصورة واضحة في اعتماد جل المؤسسات الحكومية و الخاصة على تقنية المعلوماتية، لما لها من قدرة هائلة تجعلها قادرة على عملية جمع و تخزين و معالجة، واسترجاع و مقارنة كم هائل من البيانات الخاصة بأفراد المجتمع في قطاعاته المختلفة، و لكن ما يثير القلق هو إساءة استخدام المعلومات ذات الطابع السري، التي تخزن إلكترونيا و هو قلق يزيد من حدته أن هذه المعلومات إذا ما تم الربط بينها واستعمالها فإنه يمكن أن تظهر جوانب يضر كشفها بالمصالح العامة و الشخصية للمعنيين بها.[2]

إن الإطلاع أو التعدي على المعلومات بطرق إحتيالية غير شرعية تعتمد على الاختراق عادة، و الذي يشكل كسلوك تعديا على حق الغير و يترتب أثرا مباشرا في شكل نتيجة إجرامية و مجني عليه، هذا الأخير له

[1] نهلا عبد القادر المومني- مرجع سابق- ص 86،87.

[2] بولين أنطونيوس أيوب - مرجع سابق- ص 97،98.

وضع خاص في الجرائم المعلوماتية، فالمعتدى عليه في هذا المجال هو من يكون ضحية الإعتداء غير المشروع الذي يستهدف مكونات الحاسوب المادية أو المنطقية، فقد يكون شخصا طبيعيا أو معنويا في شكل شركة حكومية أو خاصة، ويشترط لأن ينطبق عليه هذاالوصف أن يكون الإعتداء قد استهدف المجني عليه في إحدى المكونات المادية أو المنطقية لحاسوبه أو للشبكة التي يتصل من خلالها.

و الملاحظ أنه من الصعب تحديد ضحايا الإجرام المعلوماتي على وجه الدقة لأن هؤلاء لا يعلمون شيئا عنها إلا بعد وقوعها، و في هذه الحالة يفضل أغلبهم أنه من الحكمة عدم الإبلاغ عنها وبالتالي لا يحبذ أكثرهم أن يعترف بأن نظامه المعلوماتي قد وقع ضحية إعتداء معلوماتي لما قد يشكل هذا الاعتراف من دافع المجرمين في الاستمرار في اعتدائهم.[1]

ويبدوا أحجام المجني عليه في مجال الجرائم المعلوماتية عن الإبلاغ عن الجريمة أكثر وضوحا في المؤسسات المالية مثل البنوك، حيث تخشى إدارتها أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم إلى تضاؤل الثقة فيها من قبل المتعاملين معها، و هو ما قد يؤثر سلبا في السياسة التي يمكن أن توضع لمكافحتها.[2]

وتعتبر المعلومات مجموعة من القيم المستحدثة الهدف الأول للجرائم المعلوماتية فيمكن تصور وقوع الاعتداء عليها سواء عن طريق بيعها أو مقايضتها أو إتلافها.[3]

فالمعلومات المستقاة من قبل القراصنة المعلوماتيين يمكن بيعها في السوق السوداء المعلوماتية، و خير دليل على ذلك هو السعر المحدد لرقم بطاقة ائتمان بنكية بدون الرمز السري والمساوي لـ 25 دولار أمريكي، أما سعرها مع رقمها السري فحدد بـ 500 دولار أمريكي.[4]

[1] خالد عياد الحلبي- مرجع سابق- ص 37.
[2] تركي بن عبد الرحمان المويشير- مرجع سابق- ص 21.
[3]- محمد علي العريان- مرجع سابق- ص 67.
[4] - Myriam Quéméner- Yves Charpenel – La cybercriminalité- op cit - p 13.

ويتركز الاتجاه الأساسي لجرائم المعلوماتية وفقا لتحقيق أجرته مجلةRessources Informatique أن :

- 19% من أفعال الغش المعلوماتي تستهدف البنوك.
- 16% من أفعال الغش المعلوماتي تستهدف الإرادة.
- 10% من أفعال الغش المعلوماتي تستهدف الإنتاج الصناعي.
- 10% من أفعال الغش المعلوماتي تستهدف المعلومات.

لتأتي بعد ذلك شركات التأمين والشركات الخاصة، و في واقع الأمر فإن الجريمة المعلوماتية تستهدف في المقام الأول المؤسسات المالية و التي تتحكم في القيم الرأسمالية.[1]

و على سبيل المثال فإن البنوك الأمريكية فقدت ما قيمته 90 مليون دولار كخسائر ناجمة عن السرقات التقليدية، بينما تكبدت ما قيمته 12 مليار دولار كخسائر ناتجة عن الاعتداءات المعلوماتية ، و تعتبر إسرائيل الدولة الأولى من حيث عدد الهجمات الإلكترونية ، بحيث تقدر عدد الهجمات على نظامها المعلوماتي بـ 1000 إعتداء في الدقيقة الواحدة، وقد قدر مخبر (Norton) لأمن المعلوماتي خسائر الاقتصاد العالمي بـ 110 مليار دولار أمريكي نتيجة الاعتداءات المعلوماتية.[2]

إن الوصول إلى هذا الرقم ما هو إلا دليل على تنامي الإجرام المعلوماتي و استهدافه بشكل مباشر و أساسي للنظم المعلوماتية للمؤسسات المالية باعتبارها الضحية رقم واحد ، كما يدل على حجم الأطماع الشخصية للمجرمين المعلوماتيين وقد قدم معهد (Week Research) سنة 2000 تقريرا إحصائيا يفيد

[1]- عبد العال الدريبي- مرجع سابق- ص 170.

[2]–François sopin – rapport sur l'actualité de cybercriminalité en 2012 – disponible sur internet– Date de consultation : 03/06/2014– lien directe : https://www.adacis.net/wpcontent/uploads/2012/12/ADACIS_CLUSIRA_Cybercriminalit%C3%A9_2012.pdf

تسجيل خسائر مقدرة بـ 1600 مليار دولار نتيجة الوقت الضائع الناتج عن تعطيل الأنظمة المعلوماتية بسبب الاعتداءات أي ما قيمته 3,3 % من وقت العمل.

و لعل أن التقرير الذي أعده مكتب التحقيقات الأمريكي الفيدرالي (F.B.I) بالتعاون مع مركز (Lic3) الخاص بالشكاوي في مجال الجرائم المعلوماتية، هو التقرير الأدق من عيث تقديره لحجم الخسائر بحيث قدرها سنة 2009 بـ 559.7 مليون دولار بالنسبة للاقتصاد الأمريكي أي ضعف ما سجل سنة 2008 و التي كانت تشير إلى 264 مليون دولار كخسائر، بينما قفز رقم الشكوى المتعلقة بهذه الجرائم من 275284 شكوى إلى 336655 شكوى أي نسبة زيادة مقدرة بـــــــ 22 %.[1]

أما على المستوى الوطني (الجزائر) و في مجال ذكر الإحصائيات المتعلقة بعدد ضحايا الإجرام المعلوماتي فإنه يمكن الاستشهاد ببض الأرقام التي قدمتها غرفة التحقيق على مستوى محكمة سيدي أمحمد بالجزائر العاصمة لسنة 2012 بحيث نشهد تناسق الإحصائيات الدولية و الوطنية فيما تعلق بالمؤسسات المستهدفة من قبل المجرمين المعلوماتيين، فواحد وعشرون (21) اعتداءا إلكترونيا استهدف الإدارات العمومية أي ما نسبته 60 %، بينما سجلت 07 اعتداءات ضد أنظمة شركات خاصة أي ما نسبته 20 % بينما سجلت 04 اعتداءات على أنظمة شركات خاصة أجنبية أي ما نسبته 06 % بينما سجلت حالة واحدة (01)ضد هيئات أجنبية عمومية بنسبة 03 % .

إن الإحصايات المقدمة على الصعيد الوطني لا تعبر صراحة عن حقيقة الواقع و ذلك لعدة أسباب منها عدم التبليغ عن هذه الجرائم، وكذلك عدم إكتشاف أغلبها في الوقت المناسب بسبب عدم قدرة المسؤولين على أمن الانظمة على التعامل معها بالشكل المناسب في الوقت المناسب، ولعل أن الإشكال سيتفاقم بإتاحة خدمة الجيل الثالث للهاتف النقال التي تتيح التمتع بخدمة الولوج لشبكة الأنترنت دون حدود و قيود مكانية.

و ما يمكن قوله ختاما لهذا المبحث أن مفهوم الجريمة المعلوماتية أوسع بكثير مما قد يظنه البعض، وتصب أغلب مفاهيمه في الإطار التقني بالنظر إلى طبيعة المجال المعلوماتي، و إن المجال التشريعي

---

[1] Myriam Quéméner- Yves Charpenel -– La cybercriminalité- op cit- p 11.

و بالرغم من الجهود المبذولة مازال يعاني نقصا نظرا لعدم توازن وتيرة تطور الإجرام المعلوماتي والتشريع ، فهذا الأخير يعتبر جامدا بالنظر إلى الوتيرة المتسارعة للجريمة المعلوماتية ، ولذلك كان من الموجب وضع حلول جدية و على المستوى البعيد لأجل احتواء التصورات المستقبلية للسلوك الإجرامي المعلوماتي و تكثيف الجهود على المستوى الدولي بالرغم من فارق المستويات المادية خصوصا و القضائية بين دول العالم المتقدم و دول العالم الثالث، وذلك من خلال تصور مفاهيمي موحد للجريمة المعلوماتية بحيث يتجاوز معه عراقيل تطبيق مبادئ القانون من حيث الإقليم، و يعزز من فرص تطبيق مبادئ عالمية النص الجنائي ، اما على المستوى الوطني و بالمقارنة بين الجهود الدولية و الإقليمية في مجال محاربة الجريمة المعلوماتية و الجهود الوطنية، نجد أن التشريع الجزائري يعتبر ومن الناحية القانونية دون المتوسط من حيث مستوى الحماية التي توفرها أغلب النصوص التي سنت بهدف مكافحة الجريمة المعلوماتية.

فنلاحظ غياب النصوص الدقيقة و الحديثة، كما نلاحظ غياب التناسق بين قانون العقوبات والقوانين الخاصة فالمشرع الجزائري لم يعثر على مصطلح خاص بهذا النوع من الجرائم و هو ما يؤثر على نفسية الجناة من خلال عدم اعتدادهم بالشق القانوني المنظم لهذه النشاطات الإلكترونية ، سواء منها المشروعة أو المجرمة، و بالتالي وجب توحيد المصطلحات في إطار تعزيز سياسة مكافحة هذا النوع من الجرائم باعتماد المصطلح العالمي الجريمة المعلوماتية، بدل جرائم المساس بأنظمة المعالجة الآلية للمعطيات .

المبحث الثاني: صور الجريمة المعلوماتية.

الجرائم المعلوماتية كما سبق و أن فصلنا ذلك في المبحث السابق، هي تلك الجرائم التي تتم باستخدام الحاسوب و الشبكات، أو تلك الجرائم التي تقع على الحاسوب ذاته، و تتشابه الجريمة المعلوماتية و الجريمة التقليدية من حيث المفهوم باعتبارهما يشكلان تهديدا على المصلحة العامة أو الخاصة المحمية قانونا، غير أنهما يختلفان في مواضع كثيرة تتضح خصوصا في مجال الركن المادي و الركن المعنوي الخاص بكل منهما

،فنجد أن سرقة معدات الحاسوب المادية أو تخريبها، في صورة الشاشة أو الوحدة الرئيسية، أو معدات الاتصال بالشبكة كالكوابل، يعتبر من باب الجرائم التقليدية لأنها تستهدف أموالا ذات طبيعة مادية قابلة للحيازة، عكس الجرائم الواقعة على المكونات المنطقية للحاسوب والتي تستهدف برمجياته والمعلومات المخزنة بداخله أو تلك المتداولة عبر شبكة الأنترنت، ففي هذه الحالة يكون الحاسوب الخاص بالجاني هو الوسيلة في ارتكاب الجريمة.

إن النشاط أو السلوك المادي في جرائم المعلوماتية بمفهومها الخاص يتطلب وجود بيئة إلكترونية و اتصال بشبكة الأنترنت، كما يتطلب من الجاني معرفة بتفاصيل هذا النشاط و نتائجه ،فيقوم في سبيل المثال ذلك بتجهيز الحاسوب، و يحمله ببرامج الاختراق أو يعدها بنفسها و هو ما يعبر عنه بالحالة النفسية للجاني المعلوماتي.[1]

إن الجرائم المعلوماتية هي ظاهرة إجرامية تقرع أجراس الخطر لتنبه العالم إلى حجم المخاطر التي يمكن أن تنجم عنها، وهي جرائم في نسق تطور مستمر ناهيك عن كونها جرائم ذكية وذات طبيعة و منشأ خاص، فهي تنشأ في بيئة إلكترونية، يقترفها أشخاص يميزهم الذكاء والمعرفة التقنية، مما يتسبب في خسائر للمجتمع ككل و على كل المستويات الاقتصادية و الاجتماعية و الثقافية و الأمنية، و لذلك فقد استقطبت هذه الجرائم إهتمام أغلب الدول و قد حازت على قدر مهم من الإهتمام التشريعي، و ذلك سواء على المستوى الدولي أو الداخلي النابع من جهود التعاون الدولي في مكافحة الجريمة المنظمة، فنجد وعلى سبيل المثال أن اتفاقية بودابست المؤرخة في 2001/11/23 والتي انضمت إليها أغلب دول الإتحاد الأوروبي إضافة إلى 17 عشر دولة خارج الإقليم الأوروبي تجرم في قسمها الأول من بابها الثاني في نصوص المواد من 02 إلى 13 مختلف صور الجرائم المعلوماتية والتي يجب على الدول الموقعة الالتزام بتجريمها ضمن نصوصها الداخلية، و قد

---

[1] محمد على قطب- "الجرائم المعلوماتية وطرق مواجهتها" - الجزء الأول - مرجع سابق- ص 06.

أكدت المذاكرة التفسيرية بان الهدف من القسم الأول من الباب الثاني لهذه الاتفاقية هو تحسين وإصلاح وسائل منع و قمع الإجرام المعلوماتي.[1]

وهو ما تضمنه الفصل الثاني من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المؤرخة في 2010/12/21 بالقاهرة ، بعد الإجتماع المشترك لوزراء الداخلية و العدل العرب بمقر الأمانة العامة للجامعة العربية و الذي صادقت عليه إثنان و عشرون (22) دولة عربية في اليوم نفسه.[2]

إن هذا الدفع الدولي المتعلق بتجريم بعض صور السلوكات الإلكترونية بوصفها جرائم قد دفع بالمشرع الجزائري و في ظل المناخ الإلكتروني الذي أضحى يميز الجزائر إلى الإقرار بتجريم هذه السلوكات وذلك تحت وصف الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات وذلك من خلال القانون رقم 04-05 المؤرخ في 10 نوفمبر 2004 [3] , والمتضمن تعديل قانون العقوبات في قسمه السابع مكرر، و الذي أستحدثت بموجبه نصوص المواده من 394 مكرر إلى 394 مكرر 07، و لعل أن ما يمكن استخلاصه من خلال الرجوع إلى نصوص المواد السالفة الذكر سواء منها الدولية أو الوطنية، هو استقرارها على فكرة محاربة الجرائم التي تتميز بالخطورة و التي تشكل تهديدا جادا على أمن و سلامة الأنظمة المعلوماتية، و بالمقابل استبعاد بعض الجرائم البسيطة التافهة و الجرائم التي سنستعرضها في هذا المبحث هي ثلاث طوائف أساسية وهي:

جرائم تستهدف النظم المعلوماتية (المطلب الأول): أي تلك الجرائم التي تستهدف النظم المعلوماتية بصفة مباشرة، وتعتمد أسلوب الاختراق و استعمال برامج خاصة لأجل تعطيل و إتلاف المعلومات.

جرائم تستهدف المال المعلوماتي (المطلب الثاني): تلك الجرائم التي تستهدف النظم المعلوماتية بهدف تحقيق الربح ، و لعل ان أبرزها هي جرائم الإستعمال غير المشروع لبطاقات الدفع الإلكتروني.

---

[1]- هلالي عبد اللاه أحمد- مرجع سابق- ص 33.

[2]- لمزيد من التفصيل حول مضمون الإتفاقية العربية لمكافحة الجريمة المعلوماتية أنظر الملحق رقم : **04**

[3]- القانون رقم 04-05 المؤرخ في 10 نوفمبر 2004 والمتضمن تعديل قانون العقوبات، المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية العدد رقم : 71 لسنة الصادرة يوم 10 نوفمبر 2004.

جرائم تستهدف الأشخاص (المطلب الثالث): تلك الجرائم التي تستهدف المعطيات و البيانات الخاصة بحياة الأفراد فتمسهم بالقذف أو السب أو التشهير و قد تستهدف فئة ضعيفة كالأطفال.

إذن فما هي الصور القانونية لهذه السلوكات الإجرامية ذات الطابع الإلكتروني؟

المطلب الأول: جرائم التعدي على النظم المعلوماتية.

يقصد بالنظم المعلوماتية أي نظام منفصل أو مجموعة من الأنظمة المتصلة بعضهما البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذ للبرنامج.[1]

كما يقصد بالجرائم المعلوماتية بأنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.[2]

إن التعريف المقترح من قبل المشرع الجزائري لمفهوم الجريمة المعلوماتية و النظم المعلوماتية يندرج و يتسم بالشمولية في إطار تحديد مفهوم جرائم التعدي على النظم المعلوماتية، و هو ما يستلزم الرجوع إلى أحكام قانون العقوبات من أجل إيضاح معناها الخاص، و هو ما تفردت بتوضيحه أكثر نصوص المواد 394 مكرر إلى 394 مكرر 07 من القانون 04- 05 المعدل و المتمم لأحكام قانون العقوبات، التي بينت صور و أشكال الجريمة المعلوماتية وخصوصا تلك المتعلقة بالمساس المباشر بالنظم المعلوماتية، فقد بينت المادة 394 مكرر من القانون سالف الذكر، بان جرائم المساس بأنظمة المعالجة الآلية للمعطيات محددة وعلى سبيل الحصر في الصور الإجرامية التالية:

- الدخول أو محاولة الدخول بطريق الغش لمنظومة معالجة آلية للمعطيات.
- الدخول أو البقاء أو محاولة ذلك بطريق الغش لمنظومة معالجة آلية للمعطيات.

---

[1]- المادة 02 الفقرة ب- القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها.

[2]- المادة 02- الفقرة -أ- القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال و مكافحتها.

و قد عاقب عليها النص بالحبس من 03 أشهر إلى 1 سنة و بغرامة مقدارها من 50.000 دج إلى 100.000 دج و قد شدد على مسألة ضرورة مضاعفة العقوبة في حال ترتب عن هذا الفعل حذف أو تغير للمعطيات المعلوماتية، و قد و ضح المشرع أكثر صور هذا الفعل في النص الموالي 394 مكرر 01 ق 04-05 من قانون العقوبات.

وبذلك فإن النهج التجريمي المتبع من قبل المشرع الجزائري كان واضحا وشاملا، غير أن ما يطرح الإشكال بهذا الخصوص هو غياب تحديد معاني الركن المادي و المعنوي بشكل دقيق كما سنبينه لاحقا، مما قد يرتب أثارا إيجابية بالنسبة للمجرمين الذين تسمح لهم الثغرات القانونية بالإفلات من العقاب، و على كل حال فإن جرائم التعدي على النظم المعلوماتية يمكن حصرها في الصور التالية:

- جرائم الاختراق (الفرع الأول).
- جرائم إتلاف المعطيات (الفرع الثاني).
- جرائم إساءة استخدام المعلوماتية (الفرع الثالث).

الفرع الأول: جرائم الدخول و البقاء غير المشروع للنظم المعلوماتية-جرائم الاختراق.

تعتبر هذه الجرائم الأكثر شيوعا في مجال الإجرام المعلوماتي ، و السلوك الإجرامي المحبب و المفضل لمجرمي المعلوماتية ، و سنتناول بالتفصيل كل صورة من هذه الصور الإجرامية على حدى وفق ما يلي :

الفقرة الأولى: طبيعة جرائم الاختراق المعلوماتي.

تعرف جرائم الدخول و البقاء غير المشروع ، أو جرائم اختراق النظم المعلوماتية بشكل عام بأنها: القدرة على الوصول لهدف معين بطريقة غير مشروعة (بطريقة الغش)، عن طريق ثغرات في نظام الحماية الخاص

بالهدف، وهي سمة سيئة يتسم بها المخترق، لقدرته على دخول أنظمة الآخرين عنوة ودون رغبة منهم ودون علمهم بغض النظر عن الأضرار التي قد تحدثها، وتعد هذه الأنشطة الجرمية الأكثر انتشارا.[1]

ويعد الدخول و البقاء غير المشروع أو غير المصرح به للنظم المعلوماتية، سابقة ضرورية كنشاط إجرامي لأجل ارتكاب جرائم معلوماتية أخرى كإتلاف المعطيات أو سرقتها، أو التحايل الإلكتروني أو التعدي على الأشخاص غير أن مرتكب هذا الفعل قد يقصده دون سواه وهو ما أثار خلافا بين الفئة حول مدى انطباق وصف الجريمة المعلوماتية على هذا النوع من السلوكات و يمكن تخليص موقف الفقه في الاتجاهات التالية:

أولا: الإتجاه الداعي إلى عدم تجريم هذا النوع من السلوكات : يرى أنصار هذا الاتجاه أنه ومن غير الداعي إلى تجريم مجرد الدخول أو البقاء داخل النظام المعلوماتي، و خاصة إذا لم لكن الفاعل نية ارتكاب جرائم لاحقة.

ثانيا: الإتجاه الداعي إلى ضرورة تجريم فعل الدخول والبقاء غير المشروع : يرى أنصاره حتمية تجريم هذه السلوكات حتى ولو لم يكن لدى الفاعل نية ارتكاب جرائم لاحقة، مستندين في ذلك إلى حجم الخسائر المادية التي قد تترب على مجرد حالة الدخول غير المشروع أو حتى محاولة ذلك، مستهدفين بالخسائر التي لحقت بأحد المصانع الأمريكية المتخصصة في صناعة الأسلحة النووية و التي بلغت 100.00 دولار كتكلفة أبحاث بهدف منع أحد الأشخاص من الدخول إلى نظمها المعلوماتية بصفة متكررة.[2]

ولعل أن هذا الاتجاه هو الأكثر شيوعا و عملا به من قبل أغلب التشريعات التي لا ترى في وجوب تحليل نية المخترق في ارتكاب جرائم لاحقة، أمرا ضروريا لأجل تجريم الدخول غير المشروع كما هو عليه الحال في التشريع الجزائري حسب نص المادة 394 مكرر– ق 04–05 قانون عقوبات جزائري تقابلها المادة 323–1 قانون عقوبات فرنسي.[3]

---

[1] خالد عياد الحلبي- مرجع سابق ص 89.

[2]– نهلا عبد القادر المومني – مرجع سابق– ص156،157.

[3]– تشير الإحصائيات في فرنسا إلى تنامي هذا النوع من الجرائم بحيث قفزت من 419 جريمة سنة 2009 إلى 1427 جريمة سنة 2012. أنظر في ذلك : تقرير مجموعة العمل الحكومية المشتركة الفرنسية 2014– مرجع سابق– ص 20.

الفقرة الثانية: أساليب و دوافع جرائم الاختراق المعلوماتي .

يعتمد المجرم المعلوماتي أساليب معلوماتية متنوعة لأغراض إجرامية ، مدفوعا بأغراض و دوافع شخصية تنبأ عن ميولاته الإجرامية ، و يمكن ذكر أهم أساليب الإجرامية و حصرها في :

أولا- أساليبها:يعتمد هذا النوع من السلوكات على مبدأ التواصل غير المصرح به مع نظام الحاسوب أو شبكة المعلومات، من خلال استخدام وسيلة اتصال عن بعد، أو خلال التواصل عبر نقاط الاتصال الموجودة على الشبكة للدخول إلى نظام حاسوب معين، بغرض الإطلاع على البيانات أو البرامج المخزنة فيه، و يتطلب ذلك عادة تجاوز أو كسر إجراءات الحماية المعلوماتية للنظام.[1]

كما يعتمد المخترقون عادة على خطط أخرى لأجل تنفيذ أفعالهم وهي محاولة السيطرة على جدران الحماية (fire wall) و كذلك الهجوم على خادم الملفات العامة (serveur) ، وقد يستعمل المخترق طرق غير هجومية عن طريق الدخول كمستعمل عادي حائز على التصريح، ثم الولوج إلى شبكة المنشأة ثم الاتصال بالخادم و الحصول على المعلومات.[2]

وعلى كل حال فإن محترفي هذه الأنشطة يسعون دائما للإطلاع على معلومات محمية و مشمولة بالسرية، دون أن ننسى الأهداف اللاحقة التي يمكن أن تتجسد في إتلاف أو إزالة أو استغلال هذه المعلومات بشكل غير شرعي.

ثانيا : دوافعها: لجرائم الاختراق دوافع و أسباب عدة و لو أن العبث و قضاء وقت الفراغ يعد من أبرز عوامل نشوء هذه الظاهرة الإجرامية و بروزها للوجود، غير أن خبراء الأمن المعلوماتي لخصوا دوافعها في ثلاث نقاط :

[1]- خالد عياد الحلبي- مرجع سابق- ص 89.
[2] عبد الله بن سعود بن محمد السراني- مرجع سابق- ص 31.

1. **الدافع العسكري:** إن الاعتماد شبه الكامل على أنظمة الحاسوب في المجال العسكري و الصراع القائم بين الدول في مجال الدفاع فتح الطريق أمام ظاهرة الاختراق المعلوماتي بهدف التجسس لتوفير المعلومات السرية السياسية العسكرية والاقتصادية.[1]
2. **الدافع التجاري:** كما هو الحال بالنسبة للصراع بين الدول، تعيش الشركات التجارية حربا مشتعلة في مجال المنافسة وهو ما يجعلها عرضة لمحاولات الاختراق يوميا.
3. **الدافع الشخصي:** ويشكل هذا الدافع نوعا من أساليب التباهي بالنجاح في اختراق أنظمة الحاسوب، وهو الدافع المشترك عموما بين فئة طلاب الجامعات و المهتمين بمجال المعلوماتية.[2]

الفقرة الثالثة: أركان جريمة الإختراق المعلوماتي.

تقوم جرائم الدخول غير المشروع والبقاء، على مبدأ عدم إحداث أي تأثير سلبي على الأنظمة المعلوماتية، ويقوم بهذا النوع من الأنشطة ما يطلق عليهم المخترقون ذوي القبعات البيضاء، الذين يقومون بالدخول بطريقة غير مشروعة لأنظمة الحاسوب وشبكات المعلومات ومواقع الأنترنت، مستغلين الثغرات الأمنية لتلك النظم و مخترقين إجراءات الأمن المعلوماتي وذلك بهدف الوصول إلى معلومات محاطة بالخصوصية والسرية، و قد يتعدى ذلك إلى إتلاف المعلومات و هي جرائم تقوم على ركنيين أحدهما مادي و الآخر معنوي.[3]

[1]- أقدمت الولايات المتحدة الأمريكية بتاريخ 19 ماي 2014 على إعتقال خمسة (05) ضباط من الجيش الصيني ينتمون للفرقة الخاصة "61398" بتهمة التجسس المعلوماتي ، الذي إستهدف النظام المعلوماتي لست (06) شركات أمريكية كبرى في مجال الطاقة النووية و الصناعات الثقيلة ، و هو ما تسبب في فقدان معلومات غاية في السرية ، و يواجه الضباط المعتقلون عقوبة السجن لمدة 15 سنة على الأقل ، بتهمة التجسس المعلوماتي و ذلك منذ سنة 2006 و إلى غاية 2014 إنطلاقا من مقاطعة " شانغ هاي " بإستعمال معدات معلوماتية تابعة لهيئة المخابرات السرية الصينية ، و هي الحادثة التي خلفت تشنجا في العلاقات الأمريكية الصينية ، على أساس إعتبار هذه الأخيرة إعتقال ضباط من الجبش الصيني مساسا بسيادة الصين . لمزيد من التفاصيل حول الموضوع يرجى زيارة موقع جريدة :Le Figaro على الرابط الإلكتروني التالي :
http://www.lefigaro.fr/international/2014/05/19/01003-20140519ARTFIG00302-cyber-espionnage-des-officiers-de-l-armee-chinoise-poursuivis-par-les-etats-unis.php?pagination=7

[2] خالد عياد الحلبي- مرجع سابق- ص 90.

[3] محمد علي قطب- "الجرائم المعلوماتية وطرق مواجهتها" - الجزء الأول- مرجع سابق- ص07.

أولا: الركن المادي: لا يقوم الركن المادي لفعل الدخول إلى النظام المعلوماتي على مدلول الدخول المادي إلى المكان الذي يتواجد به الحاسوب ونظامه، بل هو الدخول باستخدام الوسائل الفنية والتقنية إلى النظام المعلوماتي أي الدخول الإلكتروني.[1]

ويعتبر فعل الدخول غير المشروع في نظر الفقه الفرنسي إما عن طريق التسلل إلى داخل النظام من خلال الاستعانة بتقنيات المعلوماتية، سواء في شكل برمجيات خاصة أو عن طريق الشبكة وتسخيرها لأجل عمليات الغش، وتقوم هذه الجريمة بمجرد دخول الشخص إلى نظام معلوماتي عن طريق الغش أي بدون رخصة أو تصريح إي بدون وجه حق.[2]

وتعتبر جريمة الاختراق شكيلة أي أنها تحقق بمجرد تحقق السلوك الإجرامي، إذ يلزم لتحققها نتيجة ما، وقد يترتب عليها لاحقا من أضرار بالمعطيات المعلوماتية، و التي تعتبر في نظر العديد من التشريعات ظرفا مشددا للعقاب ولو لم يكن لدى الجاني النية في تحقيق أي نتيجة.[3]

أما بالنسبة لجريمة البقاء غير المشروع داخل نظام معلوماتي فإنهما عادة ما تكون نشاطا لاحقا لجريمة الدخول غير المشروع، أو تعديا على الحق الممنوح بالدخول إلى النظام المعلوماتي من خلال تحديد مدة البقاء القصوى، ويظهر ركنها المادي على أنه نشاط مكمل لجريمة الدخول غير المشروع، ويقصد به الحالات التي يكون فيها الدخول إلى أنظمة المعالجة الآلية للمعطيات مشروعا متبوعا ببقاء غير مشروع ويتجلى ذلك في حرمان الفاعل من حق البقاء داخل النظام المعلوماتي.[4]

---

[1] نهلا عبد القادر المومني – مرجع سابق- ص 158.

[2] Myriam Quéméner- Yves Charpenel –La cybercriminalité- op cit -p 72.

[3] -خالد عياد الحلبي- مرجع سابق- ص 96.

[4]-Myriam Quéméner- Yves Charpenel – La cybercriminalité- op cit -p 73.

و يتحقق الركن المادي الجريمة البقاء غير المشروع عن طريق الصدفة، أو الخطأ، فقد يجد الشخص نفسه داخل النظام صدفة فيقرر البقاء وعدم قطع الاتصال به، ويعتبر هذه الجريمة شكلية لا تشترط تحقيق أية نتيجة كما أنها جريمة مستمرة ما استمر البقاء بصفة غير مشروعة داخل النظام المعلوماتي.[1]

ثانيا- الركن المعنوي:إن الركن المعنوي في الجريمة هنا، هو عبارة عن القصد الجنائي بعنصريه، العلم والإرادة، فالفاعل لا بد له من أن يكون على علم بأنه يقوم بفعل الدخول أو البقاء غير المشروع إلى النظام المعلوماتي، ولابد من ان تكون إرادته متجهة لارتكاب هذا الفعل.

ففعل الدخول غير المشروع أو البقاء داخل النظام المعلوماتي، يشكلان جريمة إذا ما اقترفتا بطريق الغش (Frauduleusement) وهو دليل على ضرورة توفر القصد الجنائي (العلم والإرادة)، وأن الفاعل كانت له النية في إتيان فعل مخالف للقانون، وقد أكد الفقه في فرنسا أن القصد الجنائي فيما تعلق بهذا النوع من الجرائم يتجلى من خلال الولوج إلى النظام المعلوماتي والبقاء فيه بدون وجه حق، أو بدون ترخيص من خلال حصر المسؤول عن النظام المعلوماتي لحق الدخول لأشخاص دون غيرهم، وبالتالي فإن غياب الحق في الدخول أو البقاء هو تعبير عن إرادة القائم على النظام المعلوماتي.[2]

وقد أكد ذلك المشرع الفرنسي بهذا الخصوص في نص المادة 323 قانون عقوبات فرنسي، وهو ما سار عليه المشرع الجزائري الذي اعتبر هذه الجرائم عمدية إذا ما اقترفت بطريق الغش، أي اللجوء إلى استعمال أساليب تقنية من نوع خاص تسمح للشخص الممنوع من الدخول بالدخول و البقاء في مجال إلكتروني محظور، وذلك حسب ما جاء في نص المادة 394 مكرر ق 04-05- قانون عقوبات بالقول " يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقي عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.[3]

---

[1] -نهلا عبد القادر المومني – مرجع سابق- ص 161.
[2] Myriam Quéméner- Yves Charpenel – La cybercriminalité- op cit -p 73.
[3]- لا يشترط القيام هذه الجريمة أن يكون هناك نظام دفاعي معلوماتي لتحقيق الجريمة بل يكفي لذلك أن يحدد المسؤول عن النظام المعلوماتي قائمة الأشخاص المسموح لهم بالدخول والبقاء داخل النظام المعلوماتي، وهو ما أكدته محكمة النقض الفرنسية

الفقرة الرابعة: العقوبات المقررة لجريمة إختراق النظم المعلوماتية.

بالرغم من كون هذا النوع من الجرائم ذات طابع شكلي، إلا أن أغلب التشريعات قابلتها بجزاءات عقابية حتى ولو لم يترتب عليها ضرر، وهو حال المشرع الجزائري الذي نص في مضمون المادة 394 مكرر ق 04-05 قانون عقوبات على ما يلي " يعاقب بالحبس من ثلاثة 03 أشهر إلى سنة 01 وبغرامة من 50.00 دج إلى 100.000 دج كل من يدخل أو يبقى بطريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك"

والملاحظ من خلال إستقراء الفقرة التالية من نفس المادة هو تشديد المشرع للعقوبة المقررة من خلال مضاعفتها إذا ما ترتب عن الجريمة الأولى حذف أو تغير بمعطيات المنظومة المعلوماتية، أما إذا ما ترتب عنها تخريب للنظام المعلوماتي أي تعطيله عن أداء مهامه فإن العقوبة تكون بالحبس من 06 ستة أشهر إلى سنتين 02 وغرامة من 50.000 دج إلى 150.000 دج ، كما نص المشرع في نص المادة 394 مكرر 03- ق 04-05 على تشديد العقوبة بمضاعفتها إذا ما تعلقت الجريمة بمصالح الدفاع الوطني والمؤسسات والهيئات العامة، والملاحظ أن المشرع الجزائري كان شديدا وصارما في تقرير العقوبة بالرغم من أن الجريمة شكلية، وترجع العلة في ذلك إلى الغاية المرجوة، وهي تحقيق مفهوم الردع من المنشأ، أي وضع حد لهذا النوع من السلوكات على اعتبار أنها بوابة الجرائم اللاحقة.

في 13 فيفري 2002 بمناسبة نظرها في قضية شركة(tati) ضد مسؤولي الموقع الإلكتروني (kitetur) بتهمة الولوج غير المشروع لقاعدة بيانات شركة (tati) والذي أكد فيه دفاع المتهم أن الدخول كان بسبب غياب وسائل الحماية وبالتالي فهو نظام مفتوح، غير أن المحكمة رفضت هذا الطرح بالقول:" ضعف الحماية الأمنية للنظم المعلوماتية لا يمكن بأي حال من الاحوال أن يشكل حجة أو سببا من أجل تبرير الدخول إلى النظم المعلوماتية"

وقد عدلت محكمة الاستئناف بباريس بتاريخ 2002/10/30 مضمون هذا الاجتهاد بقولها" الدخول أو البقاء داخل جزء من النظام المعلوماتي عن طريق الاستعمال العادي لمحركات البحث لا يشكل جريمة اختراق أو بقاء غير مشروع ،و هو ما يخرج من نطاق تطبيق المادة 323 فالعقوبات فرنسي أنظر في ذلك:

Myriam Quéméner- Yves Charpenel –La cybercriminalité - op cit-p 74.

يقابل نص المادة 394 مكرر ق 04-05 قانون عقوبات جزائري نص المادة 323-1 قانون عقوبات فرنسي التي تقر بعقوبة الحبس لمدة سنتين دون تحديدها كحد أدنى أو أقصى، وبغرامة قدرها 60.000 أرو لمجرد ارتكاب هذه الأفعال، وهي عقوبات مشددة مقارنة بما جاء في نص المادة 394 مكرر ق 04-05 قانون عقوبات جزائري ، ويرجع السبب أساسا إلى مدى انتشار تقنية المعلوماتية في هذه الدولة وإلى مدى وبالتالي مدى الضرر الذي قد تلحقه هذه السلوكات بالسير الحسن للمؤسسات الفرنسية.

أما من ناحية التشريعات العربية المقارنة فإن المشرع السعودي قد نص في المادة 07 من قانون مكافحة جرائم المعلوماتية، على عقوبات شديدة مقدارها 10 سنوات سجنا وبغرامة قدرها 05 ملايين ريـال سعودي ضد كل شخص يرتكب مثل هذه الأفعال لأجل الحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني.

إذن ما يمكن استخلاصه أن جرائم الاختراق المعلوماتي وبالرغم من طابعها الشكلي نظرا لارتباطها بمظاهر إجرامية لاحقة تعتبر أشد خطورة، ضف إلى ذلك طابع الخصوصية و السرية الذي يحيط بالمعلومات المتحصلة بطريق الغش والتي يمكن أن تستعمل ضد المصالح الحيوية للدولة.

الفرع الثاني: جرائم الإتلاف المعلوماتي- إتلاف المعطيات.

بعد تعرضنا لجرائم الدخول والبقاء غير المشروع داخل النظم المعلوماتية، نستعرض نوعا آخر من الجرائم المعلوماتية يعرف بوصف جرائم الإتلاف المعلوماتي، والتي تعتبر عادة نتيجة حتمية للجريمة الأولى فما هي يا ترى طبيعة هذه الجريمة.

الفقرة الأولى: تعريف جرائم الإتلاف المعلوماتي .

قد نلتبس ونحن نعرف جرائم إتلاف النظم المعلوماتية لما قد ما يتبادر للذهن بأننا الجرائم التي تقع على الحاسوب بمكوناته المادية أو الشبكة المتصلة بها.

فالمقصود بهذه الأخيرة هي تلك الجرائم التي ينتج عنها إتلاف المكونات المادية كالإتلاف الذي يقع على الشاشة أو الطابعة أو الأقراص المضغوطة، أو أسلاك ربط الشبكة، وهذه الصورة تنطبق عليها نصوص قانون العقوبات التقليدية التي تتناول بالتجريم فعل الإتلاف الذي يؤدي إلى إلحاق الضرر بالمال المنقول.[1]

أما جرائم الإتلاف المعلوماتي فهي كما وضحتها المذكرة التفسيرية لاتفاقية بودابست لسنة 2001 بأنها، "تخريب نظم الحاسوب بهدف الإعاقة العمدية للاستخدام الشرعي للنظم المعلوماتية بما في ذلك نظم الإتصالات بإستخدام أو التأثير على بيانات الحاسوب" ، ومصطلح الإعاقة يرتبط بالأفعال التي تحمل اعتداءا على حسن تشغيل نظام الحاسوب، وهذه الإعاقة تكون ناجمة عن إدخال أو نقل أو محو أو إتلاف أو طمس أو الإضرار بالبيانات المعلوماتية.[2]

ولقد أورد المشرع الجزائري تعريفا لهذا النوع من الجرائم وذلك وقف ما نص عليه في المادة 394 مكرر 01- ق 04-05 قانون عقوبات جزائري بالقول : " يعاقب بالحبس من 06 من ستة أشهر إلى ثلاثة سنوات 03 وبغرامة من 50.000 إلى 200.000 دج كل من أدخل بطريق الغش معطيات في نظام أو أزال أو عدل بطريق الغش المعطيات التي تضمنها" ، وهو التعريف الوارد في نص المادة 323- 2 و3 من قانون العقوبات الفرنسي التي نصت على عقاب كل شخص يتسبب في إعاقة أو منع السير العادي لنظم المعالجة الآلية للمعلومات بعقوبة مقدارها الحبس لمدة 05 سنوات بغرامة مقدارها 150.000أورو ذلك من خلال الإضافة أو الحذف وما يمكن استخلاصه من التعريفين السابقين أن طبيعة هذه الجرائم ترتكز على أسلوبين أساسيين هما: إعاقة سير النظم المعلوماتية و المساس بسلامة المعلومات.

[1] نهلا عبد القادر المومني- مرجع سابق- ص 123.
[2] هلالي عبد اللاه احمد- مرجع سابق- ص 76-77.

الفقرة الثانية : الركن المادي لجريمة الإتلاف المعلوماتي.

لجريمة الإتلاف المعلوماتي و على غرار الجرائم الأخرى الخاضعة لمبدأ شرعية الجرائم و العقوبات ، ركن مادي تقوم عليه الجريمة و ذلك بالرغم من الطابع المنطقي لها و صور الركن المادي لهذه الجريمة هي :

أولا : إعاقة السير العادي للنظم المعلوماتية : أولا نشير إلى أن المشرع لم يتعرض في نص 394 مكرر 01 ق 04-05 قانون عقوبات جزائري، إلى مفهوم إعاقة السير العادي للنظم المعلوماتية ، وهو السلوك الإجرامي الذي أولته اتفاقية بودابست أهمية بالغة و قد تجلى ذلك في نص القانون الفرنسي.

يقصد بإعاقة سير عمل النظام المعلوماتي،" ذلك الفعل الذي يسبب تباطوءا في عمل النظام أو ارتباكا، مما يؤدي إلى تغير في حالة عمل النظام على نحو يصيبه بالشلل المؤقت".[1]

ويتحقق الركن المادي لهذا النوع من الجريمة من خلال وقوع اعتداء على نظام معلوماتي يسبب ارتباكا في عمله قد يكون دائما في حال استعمال الفيروسات، أو مؤقتا يهدف إلى شل أو تعطيل النظام كما هو الحال في حالة إستعمال القنابل المنطقية، أو من خلال إغراق الخادم بالرسائل الإلكترونية لأجل الحد من قدرته على التعامل مع المعلومة.[2]

وعلى كل حال فإنه يجب أن تكون الإعاقة دون وجه حق ، وبالتالي فإن أولئك الذين تكون لهم الحق في إطار ممارسة أنشطة تصميم الشبكات أو تشغيلها وصيانتها واختبارها، لا تعتبر أنشطتهم غير شرعية إذا ما تسبب في إعاقة النظام.[(3)]

ثانيا :المساس بسلامة المعلومات : إن المساس بسلامة المعلومات Atteintes a l'intégrité des donnés كسلوك مجرم محصور في فعل الإدخال، التعديل، الحذف للمعطيات المعلوماتية المخزنة في ذاكرة

[1]- محمد أمين الشوابكة – مرجع سابق – ص 223.
[2]-Myriam Quéméner- Yves Charpenel – La cybercriminalité –op cit - p 76.
[3] هلالي عبد اللاه أحمد – مرجع سابق- ص 78 .

الحاسوب، أو على الشبكة هو ما أتفقت عليه أغلب التشريعات كما جاء في نص المادة 394 مكرر 01 ق 04-05 قانون عقوبات جزائري، المادة 323-3 قانون عقوبات فرنسي، المادة 05 من نظام مكافحة الجريمة المعلوماتية السعودي، ويقوم الركن المادي لهذه الجريمة من خلال:

1. حذف أي محو البيانات كليا وتدميرها إلكترونيا، كمحو الذاكرة الرئيسية للحاسوب، أو استعمال برمجيات خفية تعمل على محو محتوى الحاسوب أو الشبكة.

2. تعديل البرامج والمعطيات المعلوماتية من خلال:

أ- التلاعب بالبرامج أي بالنظام المعلوماتي بشكل يؤدي إلى إخفاء البيانات كليا أو جزئيا.

ب- اختلاس البرامج ويكون عن طريق نسخها عن طريق أسلوب التجسس.

ج- تغيير نظم عمل البرامج أي بتزويدها بتعليمات إضافية تتيح الوصول إلى جميع المعطيات التي يتضمنها الحاسوب.

3. إدخال برامج جديدة : أي إصطناع برنامج كامل أو ناقص في الناحية الفنية يخصص لارتكاب فعل الغش المعلوماتي.[1]

الفقرة الثالثة: الركن المعنوي لجرائم الإتلاف المعلوماتي.

يتحقق الركن المعنوي بتحقيق السلوك المادي المقترن وجوبا بالقصد الجنائي (الإرادة العمدية)، باستثناء الحالات المرخص لها إدخال تعديل أو حذف جزء من النظام المعلوماتي، ويعتبر قائما هذا الركن من لحظة إدخال أو تعديل أو حذف المعلومات المقترنة بإرادة إحداث تعديل على النظام المعلوماتي، مهما كانت النتيجة المتوقعة أو غير المتوقعة على النظام.[2]

[1] محمد أمين الشوابكة- مرجع سابق- ص 237 .

[2] Myriam Quéméner- Yves Charpenel –La cybercriminalité- op cit- p 77.

أما فيما يخص عنصر العلم فإنه يتحقق إذا ما كان الفاعل يعلم بأن المحل المعتدى عليه (النظام المعلوماتي) ملك للغير، و أن فعله بالإدخال أو الحذف والتعديل هو فعل من شأنه إحداث تلف أو إعاقة للنظام المعلوماتي عن أداء مهامه بشكل طبيعي، ولعل أن تمييز مصطلح "بواسطة الغش "Frauduleusement" في نص المادتين 394 مكرر 1 ق 04-05 من قانون العقوبات الجزائري، والمادة 323-2 و 3 من قانون العقوبات الفرنسي ما هو إلا دلالة على تأكيد المشرع بضرورة توافر القصد الجنائي لأجل قيام المسؤولية الجنائية في مجال هذا النوع من الجرائم، و بالتالي تستثني من نطلق التجريم نفس الأفعال إذا لم تقترن بنية إحداث الضرر.

الفقرة الرابعة: الوسائل الفنية لتنفيذ جرائم الإتلاف المعلوماتي.

تتنوع أساليب جرائم إتلاف المعلومات وأنماطها و لا يمكن حصرها ولا التنبؤ بمستقبلها، نظرا للنسق المتسارع لتطورها و ازدياد معدل الاعتداءات المعلوماتية من يوم لآخر فقد افادت شركة Kaspersky المختصة بالأمن المعلوماتي في تقريرها السنوي لـ 2014 بأن منتوجاتها الخاصة بالحماية نجحت في التصدي لـ6,167,233,068 مليار هجمة إلكترونية عن طريق البرماج الخبيثة [1]، وهو ما يدل على تعدد وسائل تنفيذ الاعتداءات الإلكترونية و إتاحتها أمام مجرمي المعلوماتية و يمكن حصر أو تصنيف هذه الوسائل إلى ثلاث طوائف رئيسية هي:

أولا : الفيروسات الخاصة بالحاسوب: الفيروس هو "شفرة حاسوبية"، أو برنامج ذو قدرة هائلة على التناسخ، يستطيع إلصاق نفسه ببعض الملفات و البرامج الحاسوبية، كما يملك القدرة على الانتقال من حاسوب لآخر بواسطة الشبكة، و للفيروس آثار مدمرة و في أحسن الأحوال فهي مزعجة، و قد تتسبب الفيروسات في حذف

[1] – لمزيد من التفصيل يرجى الإطلاع على التقرير السنوي لشركة **Kaspersky** لسنة 2014 المنشور على شبكة الأنترنت– تاريخ التصفح 2015/03/25 الرابط الإلكتروني :
http://www.viruslist.com/fr/analysis?pubid=200676376

كامل محتوى القرص الصلب للحاسوب ، أو تحذف بعض أجزاء نظم التشغيل المهمة أو تحتل مساحة مهمة على القرص الصلب للحاسوب فتعيق عمله.[1]

عادة ما يكون الفيروسات مرافقة و مخزنة على البرامج التطبيقية، و برامج التشغيل، و تنشط في حالة نسخ البرامج من جهاز لآخر، أو عن طريق الشبكات (الأنترنت)، فتكون مختبئة في الرسائل الإلكترونية، و قد تكون عامة العدوى أي تنتقل من برنامج لآخر و تعطل نظام تشغيل الحاسوب برمته، أو محددة العدوى أي أنها تستهدف نوعا معينا من النظم فتعطل عمل الحاسوب جزئيا[2].

و من أشهر الفيروسات الموجهة ضد الأنظمة و الحواسيب هي :

1- **فيروسات الإبطاء:** و تعمل على إبطاء الحاسوب عن العمل تمهيدا لتوقيفه.

2- **الفيروسات النائمة:** و هي فيروسات تظل منكمشة إلى حين انطلاقها، لأجل تدمير و تعطيل نظم تشغيل الحاسوب.

3- **لفيروسات التطورية:** و هي فيروسات لها القدرة على تغيير شكلها و التأقلم مع مضاد الفيروسات، تعمل على تخريب و تعطيل النظام.

4- **حصان طروادة:** تختبئ هذه الفيروسات ضمن برامج تبدو بريئة و عندما يتم تشغيلها ينشط الجزء الماكر منها ، فتقوم بممارسة عملها و هو السيطرة على الجهاز و إتلافه من خلال جمع المعلومات عن اسم المستخدم و كلمة السر و إرسالها لصاحب الفيروس ، أثناء اتصال المستخدم بالشبكة كما يسمح بتصفح الجهاز و التحكم فيه عن بعد و بملفاته بشكل كامل .[3]

ثانيا : برامج الدودة (Worm Soft wear) : هي عبارة عن برمجيات تقوم بالانتقال من حاسوب لآخر، دون الحاجة إلى تدخل الإنسان من أجل تنشيطها ، فهي تعمل بصفة خاصية التنشيط الذاتي، و بذلك فهي تختلف

---

[1] تركي بن عبد الرحمان المويشير- مرجع سابق- ص 44.
[2] محمد أمين الشوابكة – مرجع سابق- ص 239.
[3] تركي بن عبد الرحمان المويشير – مرجع سابق- ص 33.

عن الفيروسات ، كما أنها تلتصق بنظام التشغيل للحاسوب الذي تصيبه، و تسبب عادة حركة الدودة تعطيل الحاسوب ، من خلال تجميد لوحة المفاتيح أو الشاشة ، كما تعبئ الذاكرة و تبطل من عمل الحاسوب .[1]

ولعل أن أشهر أنواع الدودة المعلوماتية هي دودة موريس، التي أطلقها هذا الطالب الأمريكي روبرت موريس– Robert Morris في جامعة كورنان عام 1988 عمدا بهدف إثبات ضعف شبكة الأنترنت من حيث الأمان، و هو ما تسبب في تدمير 16 ألف شبكة عبر الولايات المتحدة الأمريكية، إضافة إلى تعطيلها لعدة أيام و قد حكم عليه بالحبس لثلاث 03 سنوات و 10500 دولار كغرامة و 400 ساعة عمل عقوبة النفع العام.[2]

–**ثالثا : القنابل المعلوماتية** : وهي نوع من البرامج الخبيثة تعمل على شكل قنبلة تقليدية، غير أنها إلكترونية ، و هي نوعان:

1–القنابل المعلوماتية المنطقية : هي عبارة عن برامج صغيرة الحجم، يتم إدخالها بطرق الغش مع برامج أخرى تهدف إلى تدمير و تغيير برامج و معلومات النظام في لحظة محددة أو خلال فترات زمنية منتظمة بحيث تعمل على مبدأ التوقيت، فتحدث دمارا أو تغيرا في المعلومات و البرامج عند إنجاز أمر معين في الحاسوب أو البرنامج من قبل المستخدم.[3]

2– القنابل المعلوماتية الزمنية: عكس الأولى فهذه تحدث دمارا و تغيرا في لحظة زمنية محددة بالساعة و اليوم و السنة، و يتم إدخالها في برنامج معين و تنفذ في جزء من الثانية، أو في ثواني أو دقائق معدودة وفقا لتاريخ محدد سلفا.[4]

---

[1] حسين فريجه- "الجرائم الإلكترونية و الأنترنت" - مقالة علمية - مجلة المعلوماتية – العدد 36- أكتوبر 2011- وكالة التطوير و التخطيط- وزارة التربية و التعليم – السعودية- ص 06. متوفرة على شبكة الأنترنت – تاريخ التصفح : 2013/06/26- الرابط الإلكتروني :

http://informatics.gov.sa/articles.php?artid=586

[2] بولين أنطونيوس أيوب – مرجع سابق – ص 180.

[3] محمد أمين الشوابكة – مرجع سابق – ص 240.

[4] محمد علي العريان – مرجع سابق – ص 99.

ففي فرنسا مثلا قام محاسب خبير في نظم المعلومات و بدافع الانتقام على إثر فصله من عمله بزرع قنبلة زمنية في شبكة المعلومات الخاصة بالمؤسسة و انفجرت بعد 06 أشهر من رحيله مما خلف تلفا كليا للبيانات المتعلقة بالشركة.[1]

كل هذه تعتبر وسائل يستعين بها مجرمو المعلوماتية بهدف تحقيق أغراضهم الإجرامية التي تتمثل عادة في إتلاف المعلومات و النظم المعلوماتية على حد سواء ، و ما ذكرنا لهذه الوسائل ماهو إلا استشهاد بأهمها و أقربها إلى فهمنا ، فهناك الآلاف من الوسائل الحديثة و المستحدثة بما يفوق مجال اختصاصنا و يتعدى إطارنا القانوني لأجل وصفها.

الفرع الثالث: جرائم إساءة استخدام المعلوماتية.

تناولت أغلب التشريعات، و الاتفاقيات سواء الدولية أو الإقليمية بتحديد المفاهيم المتعلقة بمحاربة الجريمة المعلوماتية باعتبارها سلوكا يهدد و يشجع على الاعتداء على المصالح العامة و الخاصة، في شاكلة الجرائم التقليدية (كالقتل، السرقات، الاعتداء على الغير...) ، و من المفاهيم التي تطرقت لها التشريعات هو المفهوم المتعلق بتجريم صور السلوكات التي تعتمد على إساءة استخدام النظم المعلوماتية ، نظرا لما قد تقدمه هذه السلوكات السلبية من تشجيع و تيسير للمجرمين المعلوماتيين في إتيان الأفعال المجرمة المذكورة سالفا (الدخول و البقاء غير المشروع ، الإتلاف المعلوماتي) ، على اعتبار أن هذه الجرائم تعتمد على توفير المعلومات من خلال عرضها للبيع أو إتاحتها بصفة مجانية على شبكة الأنترنت أو على وسائط تخزين خارجية، لغرض استعمالها في إتيان الجرائم المعلوماتية.

[1] بولين أنطونيوس أيوب – مرجع سابق – ص 182.

الفقرة الأولى: تعريف جرائم إساءة استخدام المعلوماتية.

وجدت هذه الجرائم مجالا تعريفيا في نصوص القانون، فقد عرفها المشرع الجزائري من خلال نص المادة 394 مكرر 02.ق 04. 05 قانون عقوبات جزائري بالقول : "يعاقب بالحبس من شهرين (02) إلى ثلاث (03) سنوات و بغرامة من 1.000.000 دج إلى 5.000.000 دج كل من يقوم عمدا أو عن طريق الغش بما يأتي :

–تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم".

ولعل أن مفهومها يتضح بشكل أفضل وفق نص المادة 09 من الاتفاقية العربية لمكافحة جرائم التقنية الحديثة بوصفها لجرائم إساءة استخدام وسائل تقنية المعلومات على أنها:

–إنتاج أو بيع أو شراء أو توزيع أو توفير:

- أية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في المواد من 06 إلى 08 من نص الاتفاقية .
- كلمة سر أو شفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد استخدامها لأي من الجرائم المبينة في المواد من 06 إلى 08 من نص الاتفاقية.
- حيازة أي أدوات أو برامج مذكورة في الفقرة أعلاه، بقصد استخدامها لغايات ارتكاب أي من الجرائم المذكورة في المواد من 06 إلى 08 من نص الاتفاقية.

و قد تعرضت اتفاقية بودابست قبل ذلك (2001) إلى تجريم هذا النوع من السلوكات باعتماد نفس الصياغة و ذلك وفق ما جاء في نص مادتها السادسة (06) ، و ما يمكن ملاحظته أن أغلب النصوص التشريعية قد نصت على تجريم أفعال إساءة استخدام الحاسوب بالرغم من أنه سلوك لا يترتب عنه أي ضرر

يمس بأمن و سلامة النظم المعلوماتية، باعتباره سلوك خارجي يتم بعيدا عنها، غير أنه و من جهة أخرى يتيح الاستفادة من الوسائل المادية أو البرمجيات لارتكاب الجرائم المعلوماتية السالفة الذكر.

أما ما يمكن استخلاصه من خلال استقراء نص المادة 394 مكرر 02 ق. 04-05 قانون عقوبات جزائري مقارنة بالنصوص السالفة الذكر، أن المشرع الجزائري لم يعتمد على الدقة بالشكل المناسب في توضيح مفهوم هذا النوع من الجرائم، فنلحظ استعماله لأوصاف متعددة تفتقر للدقة ، كوصف فعل التجميع أو البحث أو التصميم، التي تترك مجال التساؤل مفتوحا حول المقصود بهذه السلوكات أهي فعل تجميع المعلومات أو البحث عنها أو تصميمها أو تجميع الوسائل المادية أو البرامج؟ و ذلك بالرغم من أنه ربطها بفعل الغش غير أنها تظل غامضة من حيث المفهوم القانوني.

فقد كان على الأحرى على المشروع الجزائري توظيف مصطلحات تقنية قانونية أكثر دقة و شمولية و تناسبا مع موضوع التجريم، أسوة بما قدمه نظيره السعودي في نص المادة 06 من قانون مكافحة الجرائم المعلوماتية السعودي التي جاء فيها ما يلي:"يعاقب بالسجن مدة لا تزيد عن خمس 05 سنوات و بغرامة لا تزيد عن ثلاث 03 ملايين ريال أو بإحدى هاتين العقوبتين كل من ارتكب الجرائم المعلوماتية التالية:

- إنتاج ما من شأنه المساس بالنظام العام، القيم الدينية، الآداب العامة، حرمة الحياة الخاصة، أو إعداده أو إرساله أو تخزينه عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي".

و قد نرجع سبب عدم دقة النص العقابي الجزائري من حيث تحديد معالم التجريم إلى قدمه أساسا، فتاريخ سن القانون يعود إلى سنة 2004 أين كانت مفاهيم الجريمة المعلوماتية غير مستقرة بعد، و لكنه لا يعتبر سببا كافيا يمنع المشرع الجزائري من التدخل مرة أخرى بوضع قوانين حديثة متماشية و تطور الجريمة المعلوماتية.

الفقرة الثانية : أركان جريمة إساءة استخدام المعلوماتية.

تقوم هذه الجرائم على توفر عنصرين أساسيين هما:

أولا: الركن المادي: يشكل هذا السلوك الإجرامي جريمة جنائية منفصلة و مستقلة، تتمثل في ارتكاب أفعال غير مشروعة ذات طبيعة خاصة ترتبط ببعض الأجهزة أو البرامج أو بيانات الدخول، في صورة إساءة استخدامها بغرض إتاحة جرائم معلوماتية أشد و أخطر، إن ارتكاب هذه الجريمة يستلزم عادة و في غالب الأحيان حيازة وسائل الولوج مثل أدوات و برامج القرصنة أو أي وسائل أخرى بغرض استعمالها لأغراض إجرامية، الأمر الذي يؤدي في النهاية إلى خلق نوع من السوق السوداء لإنتاج و توزيع مثل هذه الأدوات كما هو عليه الحال في الفضاء السيبرني الحديث المعروف بـ (The Dark Net).[1]

و يمكن حصر الركن المادي لهذه الجريمة في تحقق السلوكات التالية:

- تصميم برامج تساعد على الدخول غير المشروع داخل النظام المعلوماتية.
- تصميم برامج تساعد على إتلاف المعلومات كبرامج الفيروسات.
- البحث و تجميع المعلومات و البرامج التي تساعد على ارتكاب الجرائم الأخرى.
- توفير و نشر كل ما من شأنه المساعدة على ارتكاب الجرائم المعلوماتية.
- الاتجار في كل وسائل ارتكاب الجرائم المعلوماتية.

ثانيا: الركن المعنوي: تعتبر هذه الجرائم ذات طابع عمدي و هو ما نستنتجه من نصوص قانون العقوبات الجزائري في نص المادة 394 مكرر 02 ق 04-05 التي أكد فيها المشرع على ضرورة توفر عنصر القصد الجنائي من خلال استخدامه لعبارة "عمدا أو عن طريق الغش" و بالتالي فإنه تستبعد من مجال التجريم الحالات التي لا يتوفر فيها القصد الجنائي أي صور الخطأ.

و على كل حال فإنه يشترط لقيام هذه الجريمة أن ترتكب عمدا و بدون وجه حق أي يتوفر القصد الجنائي العام، أضف إلى ذلك يجب توفر نية خاصة أو قصد جنائي خاص يتمثل في استخدام جهاز الحاسوب

---

[1] هلالي عبد اللاه أحمد- مرجع سابق- ص 84-85 .

و الشبكة لأجل ارتكاب الجريمة المشار إليها، و استنادا من ذلك نخرج من دائرة التجريم الأدوات و البرامج المصرح بها لأجل استخدامها من أجل اختبار أو حماية جهاز الحاسوب.[1]

الفقرة الثالثة : العقوبات المقررة لجرائم إساءة استخدام المعلوماتية : أقر المشروع الجزائري بعقاب كل من يتعمد أو يستعمل طريق الغش لأجل ارتكاب جرائم إساءة استخدام المعلوماتية بعقوبة الحبس من (02) شهرين إلى (03) سنوات و بغرامة من 1.000.000 دج إلى 5.000.000 دج و تضاعف هذه العقوبة إذا ما مست بأمن الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للنظام العام، دون الإخلال بمبدأ تطبيق عقوبات أشد إذا تعدت من حيث النتيجة أو القصد ما كان مقررا بدءا.

والملاحظ أنها عقوبات تقليدية تتراوح ما بين العقوبات البدنية و المالية لا يتعدى حدها الأقصى 03 سنوات إلا في الحالة التي تمس فيها بالمصالح العليا للبلاد فإنها تضاعف أي تصل لمدة أقصاها (06) ستة سنوات فالمشرع الجزائري حاول قمع هذه الجريمة باعتبارها نشاطا خطيرا يهدد أمن و سلامة النظم المعلوماتية خصوصا تلك الخاضعة لتحكم مؤسسات الدولة ، و إذا ما قارنها بما هو وارد في نص المادة 323-3-1 قانون عقوبات فرنسي التي جاء فيها: "أنه كل من قام و بطريق الغش، باستيراد أو حيازة، توفير، أو تنازل أو وضع تحت التصرف معدات، و وسائل و برامج معلوماتية، أو معلومات مخصصة و مكيفة لارتكاب الجرائم المنصوص عليها في المواد 323-1 إلى 323-3 يعاقب بالعقوبات المقررة للجريمة المرتكبة في حد ذاتها و في حال ارتكاب أكثر من واحدة فإنه يعاقب بالعقوبة الأشد" ، فإننا نلاحظ أن المشرع الفرنسي كان ذكيا في مجال قمع هذه الجرائم و ربطها بمدى تحقق النتيجة الإجرامية و إمكانية تحقق جرائم لاحقة عنها، و ذلك حتى يغلق باب الإتاحة المعلوماتية أساسا و لا يترك مجالا للمناورة أمام النص القانوني و يرجع السبب في ذلك إلى إتقان النظام الخاص بمكافحة الجريمة المعلوماتية و دقته عكس التشريع العقابي الجزائري الذي يحتاج إلى ثورة

[1] هلالي عبد اللاه أحمد- مرجع سابق- ص 88،89 .

قانونية يشترك فيها الفنيون القائمون على مجال النظم المعلوماتية و القانونيون على حد سواء ،من أجل تحديد دقيق لمفاهيم هذه السلوكات من الناحية الفنية و التقنية و القانونية أساسا.

المطلب الثاني: الجرائم المعلوماتية الواقعة على الأموال.

إخترنا معالجة الجرائم المعلوماتية التي تستهدف الأموال، أي تلك السلوكات ذات الطابع الاحتيالي أو التي ترتكب بطريق الغش، من خلال استعمال الحاسوب و الشبكة (الأنترنت) و التي يهدف مرتكبها إلى تحقيق مصلحة مالية، و كسب مادي غير مشروع من خلال استهداف الأنظمة المعلوماتية و التلاعب بمعطياتها و تحويل الأموال إلى حسابه الخاص ، و يثور التساؤل حول طبيعة المال المعتدى عليه و المستهدف من خلال الجريمة المعلوماتية، باعتباره لا يحمل مفهوم الأموال التقليدية ذات الطبيعة المادية، أما الجريمة المعلوماتية فهي إلكترونية لا تحمل أي صورة للفعل المادي؟

يمكن تعريف المال المعلوماتي المشمول بالحماية القانونية بأنه "كل مال إلكتروني قابل للنقل و التملك" أو بأنه "المال الموجود على الحاسوب، سواء في صورة معلومات أو بيانات إلكترونية في أي صورة كان عليها سواء كان مخزنا على أقراص صلبة أو دعامات تخزين خارجية، فهو بذلك كل المدخلات الإلكترونية التي لها من القيمة المادية مما يجعلها قابلة للتملك و تكتسي الحماية القانونية".[1]

إن الانتشار المتزايد لتقنية المعلوماتية و تداخلها مع مختلف مظاهر الحياة اليومية و بالخصوص المعاملات المالية و التجارية[2]، أدى إلى ظهور ما يعرف بجرائم الاحتيال المعلوماتي هذا السلوك الذي تعددت

[1]- نابر نبيل عمر – الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية – دار الجامعة الجديدة– مصر–سنة2012– ص32.

[2]– قدر سنة 2012 حجم مساهمة الإقتصاد الإلكتروني في فرنسا بـ 5,2 بالمئة من مجموع الدخل الخام أي بمجموع 56 مليار أورو ، و يشغل لوحده ما قدره 3,7 بالمئة من اليد العاملة أي مجموع 900,000 عامل موزع على 100,000 مؤسسة.
أنظر في ذلك : تقرير مجموعة العمل الحكومية المشتركة الفرنسية 2014– مرجع سابق– ص 07.

التعاريف بشأنه فعرفه الأستاذ الأمريكي (سكويرز– Squires) بأنه "إساءة استخدام نظام الحاسوب بحيث ينطوي كسلوك على حيلة أو خدعة مظللة".

أما تعريف المجلس الأوربي لغش الحاسوب فهو: "تغيير أو محو أو كبت معطيات أو بيانات أو برامج الحاسوب، أو أي تدخل في مجال انجاز أو معالجة البيانات من شأنه التسبب في ضرر اقتصادي أو فقد حيازة ملكية شخص آخر، أو بقصد الحصول على مكسب اقتصادي غير مشروع له أو لشخص آخر".[1]

و يعود الانتشار المتزايد لجرائم الاحتيال الإلكتروني إلى انتشار تقنية المعاملات المالية الإلكترونية خصوصا في العشر (10) سنوات الأخيرة، بفضل المزايا التي أضحت توفرها البنوك و المؤسسات المالية لزبائنها، كمزايا التوقيع الإلكتروني، خدمة الاطلاع على الرصيد عبر الخط، تبادل و نقل الأموال عبر الشبكات و النظم المعلوماتية، كل هذه الظروف أدت و بشكل منطقي إلى استقطاب اهتمام محترفي الإجرام المعلوماتي، الذين أضحت جل اهتماماتهم منصبة حول كيفيات الحصول على الأرقام السرية لزبائن البنوك أو شفرات الدخول إلى نظم المؤسسات المالية بهدف تحويل الأموال إلى حساباتهم الشخصية.[2]

و مما يدل على أن هذا النوع من الجرائم وجد ليدوم، بدوام وجود النظم المعلوماتية المالية هي الحوادث المتعددة و المتزايدة في هذا المجال و التي نشير إلى أبرزها في النقاط التاريخية التالية:

–فيفري 2007 تعرض بنك (نورديا– NORDEA) السويدي إلى سرقة ما قيمته 800.000 أورو من قبل قراصنة معلوماتيين روس و سويديين.

[1] خالد عياد الحلبي – مرجع سابق – ص 100-101 .

[2] Joël Rivière et Didier Lucas –« Criminalité et internet une arnaque à bon March » – Article publier dans la revus de la securité Globale– numero 06– année 2008– p 69–70. Disponible sur site :www.cairn.info – Fond documentaire (S.N.D.L) Système national de documentation en ligne – Algérie –Date de consultation 28/03/2014.

-مارس 2007 توقيف 150 شخص في ايطاليا بتهمة استعمالهم لأسلوب القنابل المعلوماتية و التي عادت عليهم بفوائد مالية قدرت ب 1,25 مليون أورو إضافة إلى إلقاء القبض على خمس (05) أشخاص من جنسيات شرق أوربا ساهموا في سرقة ما قيمته 1,7 مليون أورو باستعمال غير شرعي لبطاقات ائتمان بنكية.[1]

إن البعد الدولي الذي إكتسته هذه الجرائم من خلال عدم اعترافها بالحدود الجغرافية، دفع بالتشريعات إلى مكافحتها و محاولة ردعها و هو ما نجده مجسدا في نص المادة 08 من اتفاقية بودابست لسنة 2001 و المادة 11 من الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتية لسنة 2010.[2]

أما من وجهة نظر المشرع الجزائري فنجد بأنه لم يبادر إلى وضع تشريع و نص خاص محدد و دقيق المفاهيم لصور جرائم الاحتيال الإلكتروني، بل اكتفى بالإشارة إليها في نص المادة 394 مكرر02 - ق04 - 05 قانون عقوبات جزائري بمفهوم الإتجار بالمعطيات المعلوماتية عبر النظم المعلوماتية بهدف جني أرباح مالية، و بعض النصوص الخاصة كما هو الحال في نص القانون رقم 11/83 المعدل بموجب القانون 08-01 المؤرخ في 23 جانفي 2008 الخاص بالتأمينات الاجتماعية و الذي يعاقب على الاستعمال بطريق الغش لبطاقات الدفع من قبل الغير التابعة لهيئة الضمان الاجتماعي، و يرجع غياب الإطار التشريعي الخاص و الضروري الكفيل بحماية المعاملات المالية الإلكترونية إلى عدم اعتماد هذه الأساليب في مجال المعاملات المالية في الجزائر نظرا لغياب عامل الثقة بين المتعاملين و هذه التقنية نظرا لحجم المخاطر التي تهددها.

---

[1] Eugéne Kaspersky – "Défis de la cybercriminalité" – Article publié dans la revus de la securité Globale- numero 06 - année 2008- p: 22. Disponible sur site : www.carin.Info –Fond documentaire (S.N.D.L) Système national de documentation en ligne – Algérie–Date de consultation 28 /03/2014.

[2]- تنص المادة 08 من إتفاقية بودابست على أنه " تعتمد كل دولة طرف في الإتفاقية بإتخاذ التدابير التشريعية اللازمة من اجل تجريم الأفعال التالية ، إذا ما أرتكبت عمدا أو بغير وجه حق ،و تسببت في إلحاق خسارة بملكية شخص آخر عن طريق :
- إدخال ، تبديل ، محو ، بيانات الكمبيوتر.
-أي تدخل في وظيفة منظومة معلوماتية ، بقصد إحتيالي بغرض الحصول على منفعة إقتصادية لصالح الشخص ذاته او الغير."

و سنحاول استعراض أهم صور الاعتداء على الأموال المعلوماتية من خلال الفروع التالية و سنحصرها في جرائم التحويل غير الشرعي للأموال (الفرع الأول)، و جرائم الاستخدام غير المشروع لبطاقات الدفع الإلكتروني (الفرع الثاني)، و جرائم الاعتداء على المصنفات الرقمية (الفرع الثالث) .

الفرع الأول: جرائم التحويل غير المشروع للأموال أو جرائم الاحتيال الإلكتروني.

يعرف النصب أو الاحتيال على أنه من جرائم الاعتداء على ملكية مال منقول يلجأ فيها الجاني بواسطة إحدى وسائل الاحتيال المعينة قانونا، إلى حمل المجني عليه على تسليم المال المنقول، و قد عرفها آخرون بأنها الاستيلاء على الحيازة الكاملة عمدا بطريق الحيلة أو الخداع على مال مملوك للغير.[1]

و قد نص المشرع الجزائري على مفهوم جريمة النصب في نص المادة 372 من قانون العقوبات الجزائري و التي تقابلها المادة 313-1 من قانون العقوبات الفرنسي بالقول: "كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من الالتزامات أو إلى الحصول على أي منها أو شرع في ذلك، و كان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث أمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة 01 على الأقل إلى خمس 05 سنوات على الأكثر و بغرامة من 500 إلى 20.000 دج" .

إن هذا المفهوم و المطروح لجريمة النصب يتعلق بذلك الصنف من الجرائم التي يقع على الأموال المادية، و لكن هل ينطبق ذلك على مستوى النظم المعلوماتية؟

[1] محمد علي العريان – مرجع سابق – ص 123.

الفقرة الأولى: الركن المادي لجريمة الاحتيال الإلكتروني.

يقوم الركن المادي لفعل الاحتيال على فعل التظاهر والإيحاء، الذي يكون صالحا للإيقاع بالمجني عليه في الغلط، بطريقة تؤدي إلى الاقتناع المباشر بالمظهر المادي الخارجي أي أن المجني عليه في جريمة الاحتيال هو من ينخدع بهذه المظاهر و يسلم ماله للغير.[1]

والاحتيال لا يقع على الشخص الطبيعي فقط بل المعنوي أيضا، فالشركات و المؤسسات العامة و الخاصة هي من الأشخاص الاعتبارية في نظر القانون و حيث أن الحاسوب و شبكات الاتصال الداخلية و الخارجية تعد من فروع و مكونات الشركة أو المؤسسة فإنها تكون صالحة لوقوع فعل الخداع و التحايل عليها، و قد اعتبر الفقه ممارسة أفعال الاحتيال من خلال التلاعب بالبرامج و البيانات و ما يترتب على ذلك من إيهام للمجني عليه بصحتها من أساليب الاحتيال، و حسب هذا الاتجاه فإن الحاسوب ليس سوى مجرد وسيلة للتحايل ، أما الفقه الفرنسي فاعتبر أن غش الأنظمة المعلوماتية للاستيلاء على الأموال يحقق جريمة الاحتيال.[2]

و تتعامل أغلب التشريعات مع جريمة التحايل المعلوماتي وفق ثلاث (03) اتجاهات رئيسة هي:

1- تشريعات تستلزم لقيام جريمة الاحتيال أن يكون الضحية شخصا طبيعيا و من ثم لا يتصور قيام جريمة خداع الحاسوب بوصفه آلة.

2- تشريعات ترى إمكانية تطبيق النصوص الخاصة بجريمة الاحتيال على النظم المعلوماتية و هي التشريعات الأنجلوساكسونية.

3- تشريعات تطبق القواعد الخاصة بالغش و الاحتيال في مجال البريد و التلغراف و البنوك على حالة الاحتيال و النصب المعلوماتي و منها تشريع الولايات المتحدة الأمريكية.

---

[1] -تشير الإحصائيات في فرنسا إلى وقوع حوالي 28000 جريمة سنة 2012، متعلقة بالإحتيال الإلكتروني . أنظر في ذلك : تقرير مجموعة العمل الحكومية المشتركة الفرنسية 2014- مرجع سابق- ص 20.

[2] -محمد أمين الشوابكة – مرجع سابق – ص 185.

و يشترط ليتحقق الركن المادي لجريمة الاحتيال تحقق الأفعال التالية:

أولا: فعل النصب: أي تنفيذ فعل التلاعب بمدخلات النظام المعلوماتي أي تغذيته ببيانات غير صحيحة، أو من خلال التلاعب ببرامجه، إضافة إلى فعل الإدخال و الإتلاف و المحو و الطمس التي سبق و تفصيل معناها.[1]

و قد قدم مكتب التحقيقات الفيدرالي الأمريكي (FBI) مجموعة من النصائح لمستعملي الأنترنت لأجل وقاية مستعمليه من الوقوع ضحايا جرائم الاحتيال المعلوماتي و هي:

- تجنب المشاركة في المزايدات على شبكة الأنترنت إلا بعد التأكد من صحتها و دور البائع و المزايد فيها.
- عدم تقديم أرقام الضمان الاجتماعي في مجال البيع بالمزايدة على الأنترنت.
- عدم تقديم أرقام بطاقات الائتمان إلا بعد التأكد من تأمين الموقع.[2]

ثانيا: استعمال الطرق الاحتيالية: يستعين مرتكبو جرائم الاحتيال المعلوماتي بشبكة الأنترنت أساسا، من أجل تحصيل مبتغاهم و ذلك من خلال اعتماد أسلوب إرسال الرسائل الإلكترونية لضحاياهم، في شكل رسائل صادرة عن مؤسسات موثوق فيها، يطلب فيها من الضحايا المحتملين تقديم معلومات شخصية خاصة بهم، و هو ما يسمح لهؤلاء بتتبع ضحاياهم و العمل على الإيقاع بهم لأجل الاستيلاء على أموالهم، أو من خلال استعمال وسائل أكثر تطورا كتقنية (phishing) أي إرسال عناوين مواقع إلكترونية للضحايا و دعوتهم لزيارتها،و يتسبب دخولهم لها في تسرب برامج تتبع لأجهزتهم الحاسوبية تسمح للمحتالين بالحصول على كافة المعلومات الخاصة بالضحية ، و لعل أن الأسلوب الأحدث هو الاحتيال على الطريقة النيجيرية التي تعتمد على إرسال رسائل بريدية إلكترونية مفادها طلب المساعدة على تحويل العشرات من ملايين الدولارات من قبل الضحية، بدعوى أن المرسل يعاني من مشاكل سياسية في بلده الأصلي و أنه مستعد تقديم ما قيمته 10 إلى 15% من قيمة الأموال المحولة بشرط فتح حساب و تدعيمه بقيمة أولية لأجل إتمام العملية.[3]

---

1 هلالي عبد اللاه أحمد – مرجع سابق – ص 102.

2 ناير نبيل عمر – مرجع سابق – ص 84.

3 Myriam Quéméner- Yves Charpenel – La cybercriminalité – op cit – p 135.

يكتمل الركن المادي لهذه الجرائم إذا ما سبب بصفة مباشرة للغير ضررا اقتصاديا أو ماديا، أي أن يكون الجاني قد نفذ الجريمة بغية الحصول على منفعة اقتصادية غير مشروعة له أو للغير، و مصطلح الضرر الاقتصادي أو المادي واسع جدا بمفهومه فهو يشمل النقود و الأشياء المادية و غير المادية ذات القيمة الاقتصادية.[1]

الفقرة الثانية: الركن المعنوي لجريمة الاحتيال الإلكتروني.

تعتبر جريمة النصب أو الاحتيال من الجرائم العمدية، التي يتخذ فيها الركن المعنوي صورة القصد الجنائي حسب ما أورده المشرع الجزائري في نص المادة 372 قانون العقوبات، و تبعا لذلك فإنه يستلزم أن يتوافر قصد جنائي خاص يتمثل في انصراف نية الجاني إلى تملك الشيء بطريق الاحتيال.

و القصد العام في هذه الجريمة هو نتاج اجتماع عنصري العلم و الإرادة معا، فعلم الجاني بأن فعله ينطوي على الاستيلاء على هذا المال.

كما يجب أن تتحقق الجريمة بدون وجه حق، و أن تتحقق المنفعة دون حق أيضا، و بالتالي فإن المعاملات التجارية الشرعية الإلكترونية التي تتم بهدف تحقيق منفعة اقتصادية لا يعد جريمة، كالأنشطة التجارية المتعلقة بالمنافسة و التي يمكن أن تسبب ضررا اقتصاديا لشخص، و تحمل المنفعة لآخر، و التي لا يتم ممارستها بنية الغش كاستعمال برامج جمع المعلومات الخاصة بالمنافسة التجارية على شبكة الأنترنت بواسطة صائد المعلومات " Bot"، و بالتالي تستبعد الجرائم التي بنيت على أساس الغلط أو المنافسة المشروعة.[2]

و في كل الأحوال فإن المجرم المعلوماتي يعتمد أسلوبين أساسيين لأجل تنفيذ جرائم الاحتيال المعلوماتي أولهما هو: العمل على نشر و توزيع البرامج الخبيثة (الفيروسات) على أكبر و أوسع نطاق ممكن من خلال إخفائها على صفحات بعض المواقع الإلكترونية في شكل ومضات اشهارية أو مقاطع موسيقية أو فيديو

[1] هلالي عبد اللاه أحمد – مرجع سابق – ص 103.
[2] المرجع السابق – ص 105.

معروضة للتحميل مجانا، و بمجرد اطلاع المستخدم عليها يتسلل البرنامج الخبيث إلى حاسوبه و يبدأ مهمة جمع المعلومات و إرسالها إلى المجرم المعلوماتي، لتليها المرحلة الثانية و هي العمل على البقاء متخفيا لأطول مدة ممكنة من أجل جمع أكبر قدر من المعلومات، و يبقى أمر نجاح المحتال في مجال الاحتيال المعلوماتي مرهونا بمدى فطنة الضحية و قدرته على اكتشاف هذه البرامج الخبيثة.[1]

الفرع الثاني: جرائم الاستخدام غير المشروع لأدوات الدفع الإلكتروني.

تعتبر تقنية الدفع الإلكتروني للأموال من أهم التطبيقات الحديثة للمعلوماتية ، فقد كسرت حاجز التعامل بالنقود و كذلك عوائق المبادلات المالية ، فأصبحت تتم بسهولة و سيولة كبيرة و لا تستغرق من الزمن سوى لحظات ، غير انها و بقدر تطمينات المؤسسات المالية بمدى أمنها إلا أنها تبقى الهدف الأول لمجرمي المعلوماتية ، نظرا لما تدره من أرباح دون اللجوء إلى الأساليب التقليدية للسرقة و ما جاورها ، فما هي طبيعة هذه التقنية و ماهي الصور غير المشروعة لأستعمالاتها؟

الفقرة الأولى : آلية الدفع الإلكتروني و الجريمة المعلوماتية.

شاعت و انتشرت التجارة الإلكترونية التي تتيح لرجال الأعمال تجنب مشقة السفر و الانتقال من بلد لآخر من أجل لقاء شركائهم و عملائهم، و أصبح بمقدورهم توفير الوقت و الجهد و المال، كما أصبح في متناول المستهلك الحصول على ما يريده من دون التنقل أو استخدام الأموال النقدية للدفع، و كل ما يحتاجه هو جهاز حاسوب موصول بشبكة الأنترنت ، و يمكن تشبيه التجارة الإلكترونية بسوق إلكتروني يتقابل فيه البائعون و الموردون و الزبائن، و تقدم فيه الخدمات في صورة إلكترونية و يتم الدفع في مقابلها بالنقود الإلكترونية.[2]

[1] Eugéne Kaspersky – op. cit – p 25 -26.

[2] حسين فريجه – مرجع سابق – ص 04.

و قد قدرت حجم الأموال المتداولة في إطار عمليات البيع و الشراء على شبكة الأنترنت يوم 08 ديسمبر 2007 وحده 320مليون جنيه إسترليني في المملكة البريطانية مع توقع بلوغ سقف 13,5 مليار جنيه إسترليني قيمة المبادلات المالية الإلكترونية في الثلاثي الأخير لسنة 2008.[1]

إن أغلب عمليات الدفع التي تتم على شبكة الأنترنت أو بواسطة آلات الصرف و السحب للأموال الموصلة بهذه الشبكة، تكون باستعمال وسائل دفع إلكترونية تعرف ببطاقات الائتمان المصرفية، و هي تلك البطاقات التي تستعمل للدفع و التي تصدرها المؤسسات المالية و التي تسمح لحاملها بسحب أو تحويل الأموال.[2]

أما المشرع الجزائري و في نفس السياق القانوني "قانون القرض و النقد" فإنه لم يضع تعريفا لهذه الوسيلة باعتبارها من أهم الوسائل التي تساهم في تسهيل رؤوس الأموال و اكتفى بالنص في المادة 69 من نفس القانون بأنه "تعتبر وسائل دفع كل الأدوات التي تمكن كل شخص من تحويل أموال مهما يكن السند التقني المستعمل" و ذلك دون الإشارة إلى مفهوم السند التقني بالتحديد و هو ما يترك المجال واسعا للتأويل حول مدلولها الخاص، و ذلك عكس ما ورد في القانون 01/08 المؤرخ في 23 جانفي 2008 المعدل و المتمم للقانون رقم 11/83 المتعلق بالتأمينات الاجتماعية و الذي أشار فيه المشرع صراحة إلى مدلول البطاقة الإلكترونية، مع ترك الحرية كاملة لهيئة الضمان الاجتماعي فيما تعلق بتسميتها و تعريفها و تحديد شروط تسليمها و استعمالها و تجديدها و تحيينها، ما عدا ذلك فإننا لا نجد في النصوص التشريعية أحكاما خاصة بمسائل الدفع الإلكتروني بالرغم من شيوع استخدامها.

---

[1] Charlie Abrahams – « La Cybercriminalité un Business Croissant lié à l'éffondrement des crédits » – Article publier dans la revus de la securité Globale– numero 06– année 2008 -p 30 Disponible sur site : www.carin.info – Fond documentaire (S.N.D.L) Système national de documentation en ligne – Algérie– Date de consultation 28 /03/2014.

[2] قانون النقد الفرنسي المادة: 1 – 132.

الفقرة الثانية: طبيعة عمل و أنواع بطاقات الدفع الإلكتروني.

توفر البطاقات الخاصة بالدفع الإلكتروني خاصية التعامل بالأموال في شكلها الإلكتروني دون عناء التنقل لتسليمها أو تسلمها في سبيل إتمام المعاملات ، و هو ما عزز نطاق المعاملات التجارية حول العالم ، و تتخذ البطاقات الخاصة بالدفع الإلكتروني لأشكالا و انوعا عديدة ، و ذلك كنتيجة لشيوع إستعمالها و يمكن إيجاز ذلك فيما يلي :

أولا: طبيعة العمل ببطاقات الدفع الإلكتروني: يعتمد نظام عمل بطاقة الدفع الإلكتروني على عمليات التحويل الإلكتروني للأموال من حساب بطاقة العميل الخاصة بالبنك أو المؤسسة المالية المصدرة للبطاقة إلى حساب التاجر بالبنك أو المؤسسة المالية التي يوجد به حسابه من خلال شبكة التسوية الإلكترونية للهيئات الدولية، و أشهر بطاقات الدفع في هذا المجال (MASTER CARD/ VISA CARD).[1]

تعطي البطاقة خدمة الحصول على السلع و الخدمات لحاملها، بطريقتين:

الأولى: بحضور العميل بحيث يحصل التاجر على بصمة البطاقة مطبوعة على إشعار بالبيع من خلال قراءتها على جهاز (ATM) أو (DOS) مع الحصول على توقيع العميل.

الثانية: الحصول على السلع و الخدمات عن طريق تصريح كتابي أو تلفوني، بخصم القيمة على حساب البطاقة عن طريق استخدام شبكة الأنترنت.[2]

فيكفي دخول العميل إلى الموقع الإلكتروني الخاص بالتاجر على شبكة الأنترنت، ثم يختار السلع المراد شراؤها، ثم يملأ النموذج الإلكتروني بإدخال بيانات البطاقة الإلكترونية و عنوانه، و يقوم بعدها التاجر بخصم قيمة السلع من رصيد البطاقة و إرسال نسخة من الفاتورة للمشتري.[3]

---

[1] محمد أمين الشوابكة – مرجع سابق – ص 193.

[2] خالد عياد الحلبي – مرجع سابق – ص 119.

[3] محمد أمين الشوابكة – مرجع سابق – ص 193.

ثانيا: أنواع بطاقات الدفع الإلكتروني: تختلف بطاقات الدفع باختلاف طبيعتها و تصنف إلى:

1- **بطاقات الوفاء:** و هي الأكثر شيوعا و يطلق عليها بطاقات الخصم الشهري و تستخدم في الوفاء بمقابل السلع و الخدمات التي يحصل عليها حاملها من التجار المعتمدين لدى المؤسسة المالية المصدرة لها.

2- **بطاقات الائتمان:** يستطيع حاملها أن يسدد بها مجموع التزاماته مباشرة حتى و لو لم يكن يمتلك حسابا أو رصيدا لدى البنك مصدر البطاقة، و لكنه يلتزم بتسديد ما عليه من ديون تجاه ابنك في أجل محدد بالاتفاق المسبق بينه و بين البنك، و كلما سدد ديونه في الأجل المحدد تجدد الاعتماد مرة أخرى، و أشهرها هي بطاقات Visa و Master card.

3- **بطاقات الصرف الآلي:** تعطي لحاملها إمكانية سحب مبالغ نقدية من حسابه الموجود لدى البنك مصدر البطاقة بحد أقصى متفق عليه.

4- **بطاقات ضمان الشيكات:** تتيح هذه البطاقة لحاملها تحرير شيكات للمستفيد، مع تولي البنك مصدر البطاقة الوفاء بقيمة الشيكات المحررة.[1]

إن المزايا التي توفرها بطاقات الدفع الإلكتروني من تحويل للأموال، استقطبت اهتمام قراصنة المعلوماتية، حول إمكانية تخليق أرقام بطاقات بواسطة برامج تشغيل، و كذلك التقاط البيانات المخزنة عليهما عبر قنوات الأنترنت و استخدامها بصفة غير مشروعة لأجل اقتناء السلع و الخدمات مع خصم قيمتها من رصيد العملاء الشرعيين حاملي هذه البطاقة.

إذن فمجال التعدي على البطاقات لا يثار في حال سرقتها ماديا باعتبارها تخضع كجريمة لقواعد قانون العقوبات التقليدية، و لكن يثار الإشكال بخصوص الاعتداء الواقع على البيانات السرية المخزنة عليها سواء من قبل حاملها أو من قبل الغير.

[1] محمد علي قطب – الجريمة المعلوماتية و طرق مواجهتها – الجزء الثالث - بحث منشور على الموقع الإلكتروني لمركز الإعلام الأمني- أكاديمية الشرطة البحرينية- مملكة البحرين- أفريل 2011-ص08- تاريخ التصفح :2014/06/05- الرابط الإلكتروني: http://www.policemc.gov.bh/reports/2011/April/12-4-2011/634382244195974306.pdf

الفقرة الثالثة: صور الاستخدام غير المشروع لبطاقات الدفع الإلكتروني.

تمثل جرائم الاستخدام التعسفي لبطاقات الدفع الإلكتروني، أشهر الجرائم التي تستهدف الأموال المتداولة عبر النظم المعلوماتية، و خصوصا مع تنامي التجارة الإلكترونية (E–Commerce)، و تتمثل صور هذا الاستعمال التعسفي الذي يشكل جريمة في ذلك الاستعمال غير الشرعي من قبل الغير، أي من غير حامل البطاقة، لأن الجرائم التي يرتكبها حاملها يمكن أن تصنف على أنها جريمة خيانة أمانة، و يقصد بالجرائم هنا و المرتكبة من قبل الغير بأنها تلك الجرائم التي يرتكبها طائفة تهتم بمجال المعلوماتية، و تستهدف أمنها و أمر مرتاديها، فتركز جهودها على التقاط و قرصنة البيانات المالية الشخصية للأفراد أو المؤسسات البنكية من اجل إعادة استخدامها بدون وجه حق و لأجل اقتناء سلع و خدمات و تحميل الغير مسؤولية دفع مقابلها.

و تتكون بطاقة الدفع الإلكترونية من مكونين أساسيين هما:

- البطاقة نفسها.
- البيانات السرية الخاصة بحاملها.

و قد يقع فعل الاعتداء إما على البطاقة نفسها أو على مكوناتها المعنوية في إحدى الأشكال التالية :

أولا: في حال سرقة البطاقة أو ضياعها نفسها: تتخذ البطاقة الخاصة بالدفع الإلكتروني شكلا خاصا مصنوعا من مادة البلاستيك، مطبوع عليها بعض المعلومات المتعلقة بحاملها، مع شريط ممغنط يحتوي على بيانات غير مقروءة تتعلق بالبنك و العميل، فإذا ما سرقت أو ضاعت هذه البطاقة من حاملها فعليه إبلاغ البنك الذي أصدرها فورا، لمنع استعمالها من قبل الغير أو إلغائها، و هو ما ينطبق أيضا على رقمها السري، و تصبح الجهة التي سحبت منها المبالغ بعد الإخطار هي المسؤولة و يتحمل الشخص الذي عثر أو سرق هذه البطاقة مسؤولية فعل سحب المبالغ من رصيدها.[1]

[1] خالد عياد الحلبي – مرجع سابق – ص 134-135.

ثانيا: في حالة سرقة أو ضياع بيانات البطاقة: جرت العادة أن لا يمنح البنك الرقم السري الخاص بالبطاقة إلا لحاملها، حتى لا يكون عرضة للسرقة أو الاحتيال من قبل الغير و بالتالي تنحصر مسؤولية الإدلاء بأرقام البطاقة البنكية عبر شبكة الأنترنت في حاملها، كما يمكن أن يتعرض إلى سرقة رقمه السري و بيانات بطاقته من خلال ملئه لنموذج الشراء الإلكتروني على شبكة الأنترنت.[1]

كما يمكن أن يتعرض لسرقة بنياته السرية من خلال بعض الأساليب التي يعتمدها لصوص التجارة الإلكترونية و هي:

1- إنشاء موقع إلكتروني وهمي على الشبكة مطابق لموقع بعض الشركات الكبرى و استعماله في الحصول على البيانات السرية للمتعاملين ثم إغلاقه.

2- التسلل إلى مواقع الشركات التجارية و المالية و الحصول على معلومات عملائها.

3- استعمال تقنية (Mail BomBing) أي إغراق الموقع المستهدف بالرسائل البريدية و بالتالي تحميله ما لا يستوعب من معلومات مما يؤدي إلى انفجاره عبر الشبكة، و بعثرة المعلومات المخزنة فيه و منها البيانات السرية الخاصة بالعملاء.[2]

ثالثا: حالة تزوير بيانات بطاقات الائتمان: يتم تزوير بطاقات الدفع الإلكتروني على نطاق شبكة الأنترنت، من خلال تشكيل أرقام بطاقات خاصة ببنك معين، و ذلك بعد تزويد الحاسوب بالرقم الخاص بالبنك مصدر البطاقة عن طريق برامج تشغيل خاصة، و من ثم استخدام البطاقة المزورة التي لها مستخدم أصلي، و القيام بعمليات الشراء بواسطتها مما يعرض العملاء الحقيقيين لمشكلات مع البنوك بسبب استخدام بطاقاتهم،أو بطاقات مطابقة لبطاقاتهم، و هو ما يفسر اكتشاف البنوك لاعتراضات من حاملي بطاقات

[1] محمد أمين الشوابكة – مرجع سابق – ص 200.
[2] محمد علي قطب – الجريمة المعلوماتية و طرق مواجهتها – الجزء الثالث مرجع سابق – ص 12.

الدفع الإلكتروني، على عمليات لم يقوموا بها[1]، لتبين التحريات بعدها أن هذه العمليات تم إجراؤها عن طريق شبكة الأنترنت من قبل لصوص المعلوماتية الذين يستعملون تقنيات خاصة تمكنهم من الحصول على أرقام البطاقات الخاصة بالعملاء و استخدامها في عمليات البيع و الشراء.[2]

و تشير الإحصاءات في فرنسا أن:

- 71 % من الفرنسيين يقدرون بأنه ليس هناك حماية كافية عل شبكة الأنترنت.
- 75% من عنية البحث أبدوا تخوفا من عمليات الشراء عبر شبكة الأنترنت بسبب خطر قرصنة بياناتهم الشخصية ، و أغلب من فكروا في عمليات الشراء عبر الأنترنت يفضلون المواقع الفرنسية على حساب الأجنبية كمعيار ضمان.[3]

الفرع الثالث: جرائم الاعتداء على حقوق الملكية الفكرية.

مع تقدم عصر الثورة المعلوماتية، طفت إلى السطح تحديات تتناسب مع هذا التطور، فقد برزت مشاكل التعامل مع نوع جديد من أنواع الملكية الفكرية يمكن وصفها بالملكية الرقمية، و هي تلك الملكية التي تنصب على برامج الحاسوب و بياناتها و المصنفات الرقمية المنشورة على شبكة الأنترنت، التي بذل في إنتاجها و جمعها و إظهارها جهد فكري إبداعي جعل من الواجب حمايتها، كحق ملكية فردية و جماعية صاحبها كمؤلف، إن مسيرة التحول نحو مجتمع المعلومات تقضي السماح للأفراد بالنفاذ إلى هذه المعلومات مع كفالة حماية حقوق المؤلفين بمظاهر حماية حديثة تشمل الملكية الرقمية.[4]

---

[1]– شهدت سنة 2012 في فرنسا تسجيل 767,000 ألف حالة إعتراض على عمليات دفع إلكتروني عن طريق بطاقات الإئتمان ، تعرض أصحابها لعمليات سرقة رصيد بمعدل 125 أورو للبطاقة الواحدة ، مما يشكل مجموع خسائر يقدر ما بين 413 إلى 450 مليون أورو . أنظر في ذلك : تقرير مجموعة العمل الحكومية المشتركة الفرنسية 2014– مرجع سابق– ص 25.

[2] -عبد الله بن سعود بن محمد السراني – مرجع سابق – ص 42.

[3]-Myriam Quéméner- Yves Charpenel –La cybercriminalité- op cit – p 132.

[4] -عبد الكريم عبد الله عبد الله – الحماية القانونية للملكية الفكرية على شبكة الأنترنت – دار الجامعة الجديدة – سنة 2008 – مصر – ص 249.

إن مظاهر الإجرام المعلوماتي أو الغش التي يوفرها الفضاء المعلوماتي، قد عرفت تحولات جذرية، موازية لتلك التغيرات التي طرأت على الاقتصاد الشرعي، فما تقوم به بعض الشركات باعتباره عملا شرعيا يكون كذلك بالنسبة لعصابة من المحتالين،فقد أتاحت المعلوماتية وسائل جديدة بدون حدود زمنية و لا مكانية لأجل ارتكاب جرائم متكررة تستهدف خصوصا الأموال المعلوماتية.[1]

و تعد المصنفات الرقمية تعد من قبيل الأموال المعلوماتية المشمولة بالحماية ضد صور التعدي، باعتبارها ملكا لصاحبها و لا يحق لسواه استغلالها بهدف الانتفاع بها ،فما هي يا ترى هذه المصنفات و ما هي طبيعتها التي تشكل محلا للجريمة المعلوماتية، و إلى أي مدى تحظى بالحماية الجنائية؟.

الفقرة الأولى: تعريف المصنفات الرقمية و أنواعها.

إنتقلت المصنفات الفكرية في ظل عصر المعلوماتية من صورة المنشورات الورقية التقليدية ، إلى الإلكترونية أو الرقمية المتاحة عبر الشبكة ، و هو ما جعلها عرضة لمخاطر الجريمة المعلوماتية ، بإعتبارها مصدر ربح مادي خصوصا إن كانت الأصالة و الحداثة تميزها.

أولا: تعريفها: يعرف المصنف الرقمي بأنه كل "مصنف إبداعي عقلي ينتمي إلى بيئة تقنية المعلومات" فبرنامج الحاسوب مصنف رقمي، و كذلك قاعدة البيانات و طبوغرافيا الدوائر المتكاملة باعتبارها نتائج تطور علم الحاسوب، بخلاف أسماء و عناوين الأنترنت و البريد الإلكتروني التي تعتبر من المصنفات التي ارتبط ظهورها بشبكة الأنترنت.[2]

و تتصف المصنفات عموما بطابع الأصالة إما من حيث الإنشاء أو التعبير، أي أنه نتاج ذهني بطابع معين يبرز شخصية صاحبه سواء في مضمون و جوهر الفكرة أو في مجرد طريقة عرضها.[3]

---

[1] Joël Rivière et Dider Lucas – op .cit – p 68.

[2] يوسف مسعودي –" النظام القانوني لحماية المصنفات الرقمية " – مقالة علمية- مجلة الدراسات القانونية – العدد 04 – أوت 2009- مركز البصيرة للبحوث و الاستشارات و الخدمات التعليمية – الجزائر – ص 113.

[3] محمد حسين منصور – المسؤولية الإلكترونية – دار الجامعة الجديدة – مصر -2003 – ص 216.

ثانيا: أنواع المصنفات الرقمية: يمكن حصر تعداد أهم المصنفات الرقمية على النحو التالي:

1- برامج الحاسوب: و يقصد بها برامج التشغيل مثال برنامج (Windows 07) و كذلك البرامج التطبيقية كبرنامج معالجة النصوص الشهير(Windows Word) و قد أثارت البرامج الحاسوبية جدلا واسعا بين الفقهاء بين من نادى بإلحاقها بأنظمة الحماية الخاصة بحقوق المؤلف، و بين من نادى بإلحاقها بمبادئ الحماية الخاصة ببراءات الإختراع.

2- **قواعد البيانات:**و هي تجميع مميز للبيانات و المعلومات يتوافر فيه عنصر الابتكار و الترتيب، عبر مجهود شخصي يكون مخزنا بواسطة الحاسوب و يمكن استرجاعه من ذاكرته أو من خلال شبكة الأنترنت.

3-التصاميم الشكلية للدوائر المتكاملة: و هي عبارة عن رقائق إلكترونية صغيرة جدا تؤدي وظائف إلكترونية، تدمج على الشرائح الإلكترونية للحاسوب لأجل تطوير أداءه.

4-عناوين الأنترنت: تعتبر مواقع الأنترنت أحد أهم المصنفات الرقمية الناشئة في بيئة الأنترنت، و حتى الآن لا توجد تشريعات شاملة تنظم مسائل أسماء النطاقات، و الإشكال يطرح عندما يكون الاسم مطابقا لاسم تجاري أو علامة تجارية.

5-**محتوى مواقع الأنترنت:** و هي كل المحتويات المنظمة داخل موقع الأنترنت سواء مواد مكتوبة أو مرئية أو مسموعة.[1]

و قد أشار المشرع الجزائري إلى مفهوم المصنفات الرقمية في الأمر 03-08 المؤرخ في 2003/07/19 في نصوص المواد 02-03-04-05 المتضمن لقانون حماية الدوائر الشكلية و المتكاملة، إضافة إلى نص المادة 03 و المادة 27 من الأمر 03-05 المؤرخ في 2003/07/19 المتضمن قانون حماية المصنفات و حقوق المؤلف ، و اشترط المشرع لا تكون هذه المصنفات محل حماية قانونية توفر شرطين هما:

---

[1] يوسف مسعودي – مرجع سابق – ص 116.

- إفراغ الإنتاج الذهني في صورة مادية.
- إصباغ صفة الابتكار على المصنف.

الفقرة الثانية: صور الجرائم المعلوماتية الواقعة على المصنفات الرقمية.

اهتمت غالب التشريعات بوضع نصوص تجرم المساس بالحقوق المعنوية و الفكرية للغير، و بالتالي تضمن للمصنفات الحماية القانونية اللازمة، و منها المصنفات الرقمية من كافة أنواع الاعتداءات، و هو ما تكلفت به و على نحو مفصل و دقيق اتفاقية بودابست لمكافحة الجريمة المعلوماتية في نص مادتها العاشرة (10)، و هو ما دعمته المادة 17 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010. [1]

و هي الجهود التي توجها المشرع الجزائري بأحكام الأوامر 03-05- و 03-08 المتعلقة بحماية حقوق المؤلف و التصاميم الشكلية و الدوائر المتكاملة الصادرين بتاريخ 19 جويلية 2003، و هي النصوص التي يقابلها قانون حماية حقوق المؤلف الفرنسي، إن كل هذه النصوص تجسد مفاهيم جرائم التعدي على المصنفات الرقمية التي يمكن حصر صورها فيما يلي:

أولا :الاعتداء على حقوق المؤلف من خلال جرائم التقليد (la contrefaçon) : جرائم التقليد هي الفعال التي تعتمد على إعادة إنتاج أو عرض، أو نشر بأية وسيلة كانت عملا فكريا من خلال التعدي على حقوق المؤلف.[2]

إن إعادة إنتاج و بث أو نشر الأعمال المحمية عبر الأنترنت بدون موافقة حائز حق المؤلف هو أمر شائع للغاية و الأعمال المحمية تشمل عموما الأعمال الأدبية و التصويرية و الموسيقية و السمعية البصرية،

---

[1]– جاءت المادة العاشرة (10) من إتفاقية بودابست تحت الفصل الرابع الموسوم بالجرائم المتعلقة بالإنتهاكات الخاصة بخقوق المؤلف و الحقوق المجاورة لها بالقول " تعتمد كل دولة طرف ما قد يلزم من التدابير التشريعية لتجريم الأفعال التالية في قانونها الوطني :

– إنتهاك حقوق الملكية الفكرية ....

–إنتهاك الحقوق المجاورة ...." و هو النص المطابق لما هو وارد في الإتفاقية العربية لمكافحة الجريمة المعلوماتية.

[2]Myriam Quéméner- Yves Charpenel – La cybercriminalité- op cit -p 145.

و جدير بالذكر أن السهولة التي يتم من خلالها عمل نسخ غير مصرح بها عن طريق التكنولوجيا الرقمية، و النطاق الذي بمقتضاه يتم إعادة إنتاجها و توزيعها هي الشبكات الإلكترونية.[1]

و هو ما قضت به المحكمة العليا الفرنسية بتاريخ 16 أكتوبر 2006 بمناسبة النظر في قضية إحدى الموظفات التي فصلت من قبل شركة "نسيان أوروبا" و التي بادرت بالانتقام من رئيس عملها من خلال نشر صور له مع صور سيارات نسيان على موقعها الإلكتروني الخاص، و هو الأمر الذي أدى تدخل الشركة المالكة لأجل حجب الموقع و سحب الصور باعتبارها صاحبة هذا العمل و أن نشر صور سياراتها هو تعدي على حقوقها الحصرية، و هو الطرح الذي أخذت به المحكمة و الذي اعتمدته في إدانة الموظفة السابقة بجنحة التقليد المتمثلة في إعادة إنتاج و نشر حقوق فكرية.[2]

و قد أخذ القانون الأمريكي الصادر سنة 1998 بتعديل قانون المؤلف برفع مستوى الحماية للمستوى الثالث، بحيث أضاف القسم 103 من القانون فصلا جديدا يحمل رقم 12 إلى 18، و ذلك باعتماد تدابير تكنولوجية تمنع أو تحد من جرائم الاعتداء على حقوق المؤلف و هي نوعان في نظره:

- النوع الأول: تدابير تكنولوجية تمنع الحصول على المصنف المحمي بموجب قانون المؤلف.
- النوع الثاني: تدابير تكنولوجية تمنع نسخ المصنف بدون ترخيص من صاحب الحق.

فجرائم المعلوماتية هي أكثر الجرائم مساسا بحق المؤلف و خصوصا جرائم التحميل غير المشروع عبر شبكة الأنترنت، فملايين المتصفحين لشبكة الأنترنت اعتادوا على تحميل الأفلام و الموسيقى دون شرائها من مصدرها الأساسي، مستغلين في ذلك برامج متخصصة في فك شفرات الحماية، و ذلك إما بغرض استعمالها الشخصي أو بغرض إعادة نشرها و طرحها للغير على شبكة الأنترنت أو للبيع على وسائط تخزين خارجية كالأقراص المضغوطة.

[1] هلالي عبد اللاه أحمد – مرجع سابق – ص 132.

[2] Jean Michel Bruguière – Le Droit de l'internet – lois contrat et usage – Edition Litec- Paris – France - 2009- p 217.

و هو الأمر الذي استدعى تدخل المحكمة العليا للولايات المتحدة الأمريكية سنة 2005 بحيث أشارت إلى أن الشركات التي تطور و تقدم برامج لتحميل الملفات يمكن محاكمتها بتهمة مساعدة متصفحي الأنترنت على انتهاك حقوق الملكية الفكرية.[1]

و ما تجدر الإشارة إليه هو تخلف أغلب التشريعات العربية عن الركب التقني الذي تبنته الولايات المتحدة الأمريكية و فرنسا و أغلب دول العالم المتقدمة في مجال محاربة الجريمة المعلوماتية الماسة بحقوق الملكية الفكرية فنجد أن عمليات النسخ و التحميل غير المشروع و المتعلقة بحقوق الغير الفكرية أمر جد شائع عند أفراد المجتمعات العربية و المجتمع الجزائري خصوصا كما تغيب بالمقابل ثقافة احترام حق الغير الفكري.

و يقوم الركن المعنوي في هذه الجرائم في حال ارتكابها عمدا و بدون وجه حق أي أنها جرائم تشترط التعمد لأجل قيام المسؤولية الجزائية، و عليه تستبعد أفعال الاستعمال المشروع لهذه الحقوق إذا تعلقت بحق الغير في الاستعمال، و دون الإخلال بحقوق المؤلف، كاستعمالها داخل إطار علمي داخل منشأة علمية، أو نسخها بمعرفة مالكها لأجل حفظها من مخاطر التلف، أو دراستها بغرض نقدها و تطويرها، أو إذا استعملت من قبل هيئات الإذاعة المقروءة أو المسموعة أو المرئية.[2]

المطلب الثالث: جرائم الاعتداء على الأفراد.

قابل الوجه المشرق لتقنية المعلوماتية، وجه سلبي يشكل خطرا و تهديدا على الحياة العامة الخاصة و الحريات الفردية، و هو موضوع مستحدث شغل مؤخرا حيزا مهما من اهتمامات العام و الخاص، خصوصا بعد ازدياد الطلب على المعلومات الشخصية من قبل مؤسسات الدولة أو المؤسسات الخاصة بل حتى من قبل الأفراد أنفسهم في ظل الاتجاه نحو مجتمع المعلومات.[3]

---

[1] عبد الكريم عبد الله عبد الله – مرجع سابق – ص 214-215.
[2] محمد حسين منصور – مرجع سابق – ص 234-235.
[3] العربي جنان – معالجة المعطيات ذات الطابع الشخصي – الحماية القانونية في التشريع المغربي و المقارن – الكتاب 2 – المملكة المغربية – 2010 – ص 19.

و يتمثل الخطر خصوصا في غايات استعمال هذه التكنولوجيا سواء كانت بصفة آلية أو دورية أو بشكل ظاهر أو خفي، مباشر أو غير مباشر من خلال تنفيذ عمليات تتمثل في جمع و تخزين و معالجة و نشر معطيات تتعلق بأشخاص طبيعيين، في شكل كتابات أو صور أو أصوات، و توفير الإمكانيات التقنية للتصرف فيها إما على حالتها الأصلية أو بعد معالجتها و بالتالي التحكم في الغايات المستوحاة منها.[1]

و الغاية التي تشكل خطرا هي تلك الغاية التي تهدف إلى المساس بالمبادئ الأساسية لحقوق و حريات الأفراد سواء العامة منها أو الخاصة، من خلال استعمال تقنية المعلوماتية و شبكة الأنترنت خصوصا، و ذلك إما بترويج ما من شأنه المساس بالأمن العام و النظام العام، أو الحقوق الشخصية للأفراد كالحق في التمتع بالخصوصية و الحرمة و الشرف، و هي التهديدات التي سنحاول معالجتها في هذا المطلب حسب التقسيم التالي ، الفرع الأول: جرائم المساس بالنظام العام، الفرع الثاني: جرائم المساس بحرمة الحياة الخاصة، الفرع الثالث: جرائم الاستغلال الجنسي للأطفال.

الفرع الأول: الجرائم الماسة بالحريات العامة.

لقد اهتم القانون دوما بمسألة حماية النظام العام من خلال تجريم كافة صور الأفعال التي من شأنها الإخلال بالمبادئ الراسخة في المجتمع، و التي تجد أصولها في مختلف القيم الاجتماعية أو الدينة أو العقائدية، إضافة إلى المبادئ التي تسعى الدولة جاهدة إلى إقرارها و الحفاظ عليها، كمسألة الأمن العام، و قد وجد مجرمو المعلوماتية في تقنيات المعلوماتية و الشبكات وسيلة فعالة لأجل التعدي على هذه القيم من خلال نشر و ترويج كل ما من شأنه أن يمس بمبادئ الغير و المجتمع عموما، أو يخل بشعورهم بالأمن، و هي الجرائم التي توصف بأنها جرائم ماسة بالآداب العامة.

---

[1]- العربي جنان -مرجع سابق – ص 09.

الفقرة الأولى: جرائم المعلوماتية الماسة بالآداب العامة.

تتلخص عموما هذه الجرائم في تلك السلوكات الماسة بالأخلاق و لو أن التعرض لجرائم الأخلاق ليس بالأمر الهين، بالنظر إلى تباين القيم الاجتماعية من مجتمع لآخر، بل و حتى بين طبقات المجتمع نفسه فما يعد انحلالا خلقيا في مجتمع ما قد يكون غير ذلك في مجتمع آخر، و جرائم الأخلاق هي تلك التي تتضمن العدوان على القيم الاجتماعية و الأخلاقية المتعارف عليها في النظم الاجتماعية.[1]

و يشترط القانون في غالبه للقول بوجود جريمة معلوماتية ماسة بالآداب العامة أن تستوفي جملة من الشروط الأساسية و هي أن تكون علنية أي أن تترتب نتائج يعترف بها القانون و يرتب عليها آثاره، إضافة إلى أن تكون معروضة على الجمهور.

و قد تعرض المشرع الجزائري لمفهوم هذه الجرائم في بعض نصوص قانون العقوبات دون أن يحدد نطاقها المتصل بتقنية المعلوماتية، إلا أنه يمكن لنا إعمال هذه النصوص على جرائم المعلوماتية بالنظر إلى عمومية و شمولية النصوص، فنجد نص المادة 333 ق.ع.ج تشير إلى عقاب كل شخص ارتكب فعلا مخلا بالحياء بصفة علنية و ذلك بالحبس من شهرين 02 إلى سنتين 02 و بغرامة من 500 إلى 2000 دج، إضافة إلى نص المادة 333 مكرر التي تنص على نفس المقدار من العقاب في حق كل من صنع أو حاز أو استورد أو سعى إلى ذلك، أو وزع أو أجر أو ألصق أو أقام معارض أو عرض أو شرع في ذلك أو باع أو شرع في البيع أو وزع أو شرع في ذلك، كل مطبوع أو محرر أو رسم أو إعلان أو صور أو لوحات زيتية أو صور فوتوغرافية أو أنتج أي شيء مخل بالحياء.

من خلال استقراء نصوص المواد السالفة الذكر نجد أن المشرع الجزائري لم يذكر بالتخصيص الجرائم التي تقع بواسطة النظم المعلوماتية و التي تستهدف المساس بالآداب العامة و إنما يمكن تطبيق نصوص هذه المواد على الجريمة المعلوماتية باعتبارها و في الوقت الراهن من أبرز الوسائل الإجرامية المستعملة من قبل

[1] عبد العال الدريبي – مرجع سابق – ص 235.

مجرمي المعلوماتية الذين وجدوا في هذه التقنية وسيلة ذات كفاءة عالية لأجل نشر إعلاناتهم الإلكترونية التي تمس بالآداب العامة، فيمكن تصنيع و تركيب الأفلام و الصور بواسطة الحاسوب، و كذلك تخزينها و تعديلها و نشرها إما على شبكة المعلومات أو على وسائط تخزين خارجية كالأقراص المضغوطة، و بالتالي إتاحتها للجمهور و التأثير على قيمهم الاجتماعية، خصوصا بالنسبة للمجتمعات العربية الإسلامية و هو الأمر الذي شددت عليه الاتفاقية العربية لمحاربة جرائم التقنية المعلوماتية وفق ما جاء في نص المادة 12 عشر منها بوصفها لهذه الجرائم بجرائم الإباحية و التي صاغها المشرع السعودي أحسن صياغة في نص المادة 06 الفقرة 10 من قانون مكافحة الجرائم المعلوماتية السعودي بقولها: يعاقب بالسجن لمدة لا تزيد عن 05 سنوات و بغرامة لا تزيد عن 03 ثلاث ملايين ريا ل ، أو بإحدى العقوبتين كل شخص يرتكب الجرائم إنتاج ما من شأنه المساس بالنظام العام أو القيم الدينية أو الآداب العامة.

إذن كان من الواجب هنا تنبيه المشرع الجزائري لأجل مسايرة المشرع السعودي و التكييف في أقرب وقت ممكن مع المعطيات و المستجدات الحديثة للسلوكات الإجرامية ووضع تشريع متناسب مع الجريمة المعلوماتية و تحديداتها.

الفقرة الثانية: الجرائم الماسة بالنظام العام.

إن التطرق لمسألة تحديد نوع هذه الجرائم، و التي تكون الجريمة المعلوماتية وسيلة أساسية في ارتكابها، أمر في غاية الصعوبة بالنظر إلى معيار الخطورة و مدى تهديدها للمصالح العامة للأفراد، غير أن أغلب التشريعات قد وضعت ترسانة قانونية عقابية في مواجهة كل ما من شأنه المساس بأمن و سلامة مواطنيها و مؤسساتها الحيوية، و قبل التطرق إلى ذلك يمكن الإشارة إلى مفهوم الجرائم المعلوماتية الماسة بالنظام العام من خلال ما أوردته المادة 15 و 16 من الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتية بشأن نوع هذه الجرائم و حصرتها فيما يلي:

- نشر أفكار و مبادئ الجماعات الإرهابية و الدعوة لها.
- تمويل العمليات الإرهابية و التدريب عليها و تسهيل الاتصالات بين المنظمات الإرهابية.
- نشر طرق صناعة المتفجرات.
- نشر النعرات و الفتن و الاعتداء على الأديان و المعتقدات.
- القيام بعمليات غسل الأموال أو نشر طرق غسل الأموال.
- الترويج للمخدرات و المؤثرات العقلية.
- الاتجار بالأشخاص و الاتجار بالأعضاء البشرية.

أما على مستوى التشريع الوطني و بالرغم من كون الجزائر من أول الدول التي أمضت على مضمون هذه الاتفاقية بتاريخ 21 ديسمبر 2010 إلا أنها لم تبذل المجهود الكافي لأجل تجريم هذه السلوكات في قانون العقوبات، و لا زلنا نعتمد على النصوص التقليدية في شاكلة نصوص المواد من 65 إلى 96 من قانون العقوبات المتعلقة بتجريم الأفعال الموصوفة بأنها جرائم تعدي على الدفاع الوطني و الاقتصاد الوطني، و جرائم التآمر ضد الدولة إضافة إلى الجرائم الإرهابية ... وغيرها من النشاطات الإجرامية، و لكن دون تحديد مظهرها الإلكتروني، و يبقى الجهد التشريعي البارز في هذا المجال هو ما تضمنته المادة394 مكرر3 ق 04-05 من قانون العقوبات الجزائري ، التي تنص على مضاعفة عقوبة مرتكب الجرائم المعلوماتية المنصوص عليها في هذا القسم إذا ما إستهدفت الأنظمة المعلوماتية الخاصة بهيئات الدفاع الوطني و الهيئات و المؤسسات الخاضعة للنظام العام ، و هو ما يعني و حسب رأينا إستثناء تطبيق نص المادة 96 من نفس القانون ، و حصر نطاق التجريم فيما تنص عليه المواد 394 مكرر إلى 394 مكرر2 من نفس القانون ، بالرغم من إمكانية تطبيق عقوبات أشد ، كل ذلك يشكل تعارضا بين النصوص و غموضا في تطبيقها ، و هو ما يستوجب علينا توجيه عناية المشرع الجزائري إلى ضرورة الإقتداء بالتوجيهات التي تقترحها الإتفاقية العربية لمكافحة جرائم تقنية المعلوماتية لوضع نصوص خاصة تسد هذا الفراغ التشريعي.

الفرع الثاني: جرائم الاعتداء على حرمة الحياة الخاصة.

الحق في احترام الحياة الخاصة أي مبدأ الخصوصية للأفراد، هو أحد الحقوق اللصيقة بالشخصية التي تثبت للإنسان لمجرد كونه إنسانا و يعتبر هذا الحق من أهم الحقوق و ذلك لما له من ارتباط وثيق بحرية الفرد، غير أن المعلوماتية بتقنياتها الحديثة المتمثلة في أجهزة الحاسوب، و الشبكات الخاصة بالاتصال العالمية منها و المحلية، و بما توفره من قدرة هائلة على جمع المعلومات و البيانات الشخصية، و تخزينها و استرجاعها و تصنيفها و تحليلها و معالجتها، و من ثم تبادلها و تناقلها دون أي عائق تقني، يشكل تهديدا حقيقيا على حق الأفراد في احترام حياتهم الخاصة خصوصا مع ظهور ما يعرف ببنوك المعلومات، و من هنا كان من الواجب التصدي للإجرام المعلوماتي الذي أصبح يشكل تهديدا صريحا على حقوق الإنسان و هو الحق في الحياة الخاصة.[1]

و يعتبر تعريف الحياة الخاصة أمرا صعبا نظرا لمفهومها الفضفاض و مع ذلك فقد حاول بعض الفقه و ضع تعريف لها على شاكلة الفقيه "مارتن–Martin" الذي قال : " هي الحق في الحياة الأسرية و الشخصية و الداخلية و الروحية لشخص عندما يعيش وراء باب مغلق" ، و أورد مؤتمر ستوكهولم الخاص برجال القانون المنعقد سنة 1967 تعريفا جاء فيه " هي الحق في أن يكون الفرد حراً و أن يعيش كما يريد دون أدنى حق للتدخل الخارجي" ، و في ظل صعوبة تحديد مفهوم الحياة الخاصة فإنه يمكن تحديد معالمها من خلال معالم الزمان و المكان و تقاليد المجتمع ، مما يعني بأن هذا الحق يختلف تبعا لإختلاف الزمان و المكان .[2]

و تشكل جرائم الاعتداء على حرمة الحياة الخاصة للأفراد جزءا مهما من النشاط الإجرامي المعلوماتي و يمكن حصر صورها في الأوصاف التالية:

---

[1] نهلا عبد القادر المومني – مرجع سابق – ص 165.

[2] أسامة أحمد المناعسة – جلال محمد القاضي – جرائم تقنية نظم المعلومات الإلكترونية-دراسة مقارنة- الطبعة الأولى- دار الثقافة للنشر و التوزيع – عمان –الأردن- 2010-ص 225.

الفقرة الأولى: جرائم القذف و التشهير عبر الأنترنت.

للشخص الحق في الشرف الذي يكفل له احترام سمعته و شرفه، و اعتباره و كرامته من التعدي و الإيذاء، و يقصد بالشرف مجموع القيم التي يضيفها الشخص على نفسه و تشكل سمعته التي تستتبع تقدير الناس له، و يتمثل الإخلال بالشرف في الحط من مكانة الإنسان و تعريضه للاحتقار و الازدراء من قبل الغير عن طريق الأقوال و التشهير أو نسب الأفعال.[1]

و تعد جرائم الذم و القدح و التحقير من أكثر الجرائم شيوعا في نطاق شبكة الأنترنت، إذا أسيء استخدامها بهدف النيل من شرف الغير و كرامته و اعتباره، ففي إطار مجتمع المعلومات الإلكترونية يجد العابثون حرية في نشر و بث رسائل تحتوي عبارات الذم و القدح و التحقير اتجاه آخرين مستهدفين بذاتهم، بصفة وجاهية أو غيابية أو بواسطة الوسائط الإلكترونية السمعية أو السمعية البصرية.[2]

و غالبا ما تقع هذه الجرائم بوصفها الحديث الإلكتروني تحت سلطة النصوص التقليدية مما يخلق إشكالا في أمر إثباتها و هو ما ينطبق على أحكام التشريع العقابي الجزائري، بحيث يخلو من نصوص تتعلق بتجريم الاعتداءات على شرف و اعتبار الأشخاص ذات الطبيعة الإلكترونية، و تبقى المواد 296،297 من قانون العقوبات مجرد نصوص توضيح الفعل المادي المكون لجريمة القذف و السب و القدح و التحقير، إضافة إلى العقوبات المقررة لها، بدون أي ربط مباشر مع تقنية المعلوماتية بالرغم من إقرار القانون رقم 04-05 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم لنصوص قانون العقوبات، و هو على عكس المشرع السعودي الذي تكفل في نصوص قانون مكافحة الجرائم المعلوماتية بإيضاح هذا النوع من الجرائم بالتفصيل كما هو نص الفقرة

---

[1] محمد حسين منصور – مرجع سابق – ص 372.

[2] محمد أمين الشوابكة – مرجع سابق – ص 31.

وقد تم تسجيل في هذا الخصوص 2300 حالة إعتداء عبر التراب الفرنسي تتضمن جرائم السب و القذف و التشهير و التحريض على الكراهية سنة 2012 ، و ذلك مقابل تسجيل 1235 حالة سنة 2010 . أنظر في ذلك : تقرير مجموعة العمل الحكومية المشتركة الفرنسية 2014– مرجع سابق– ص 20.

05 من المادة 03 من نفس القانون، و ذلك تفسيرا لما ورد في نص 14 عشر من مضمون الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتية[1]، و يمكن حصر هذه الجرائم في الأنماط و السلوكات التالية:

أولا: استهداف شخص معين بذاته بالذم و القدح و التشهير: يكون ذلك إما باستخدام البريد الإلكتروني بحيث يعمد الجاني من خلاله، إسناد مادة معينة إلى شخص ما قد يكون معنيا بذاته، بحيث نال من شرفه أو كرامته و تعرضه إلى بغض الناس و احتقارهم، خصوصا إذا ما اعتمد الجاني في ذلك على توزيع مضمون الرسالة الإلكترونية إلى عدد غير محدد من المتعاملين مع الأنترنت عن طريق رسائل البريد الإلكتروني.[2]

و قد يجد الجاني في شبكة الويب العالمية (Web) وسيلة في إسناد مادة كتابية أو صوتية أو مرئية مسيئة لشخص فتنال من شرفه و كرامته و تعرضه إلى الاحتقار و الذم من قبل الغير، كما أنها قد ترتكب عن طريق غرف المحادثة و الدردشة (Chat Rooms) و مواقع التواصل الاجتماعي على غرار موقع (Facebook) أو (Twitter) ، أو من خلال الوجاهية بفضل استعمال تقنيات الاتصال السمعي البصري التي يوفرها خدمة (Skype).[3]

ثانيا: استهداف مجموعة من الأفراد و حث الغير على كراهيتهم: يمكن أن تستهدف هذه الجرائم مجموعة من الأفراد جملة واحدة من خلال انتماءاتهم الدينية أو العقائدية أو العرقية، و هي النقطة الأساسية التي شكلت موضوع البروتوكول الإضافي لاتفاقية الجريمة الإلكترونية بشأن تجريم الأفعال ذات الطبيعة العنصرية، و التي تحرض على كراهية الأجانب و التي ترتكب عن طريق أنظمة الكمبيوتر المؤرخة في 28 جانفي 2008

---

[1] – عرفت المادة 14 من الإتفاقية العربية لمكافحة جرائم المعلوماتية جريمة الإعتداء على حرمة الحياة الخاصة بإعتبارها جريمة معلوماتية بأنها : " الإعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات ".

[2] محمد أمين الشوابكة – مرجع سابق – ص 33.

[3] – بلغ عدد مستعملي موقع التواصل الشهير " فايسبوك " حول العالم 1 مليار و 184 مليون نسمة ، شهر جانفي 2014، أنظر في ذلك : The Global Digital Statistic 2014- op cit – p 11.

أما على المستوى الوطني فقد بلغ عدد مستعملي موقع " فايسبوك " بتاريخ 31 ديسمبر 2012 : 4,111,320 مليون جزائري ، و ذلك من مجموع 5,230,000 ملايين مشترك بخدمة الأنترنت – معلومات إحصائية متوفرة على شبكة الأنترنت–تاريخ التصفح 2014/05/05– الرابط الإلكتروني:http://www.internetworldstats.com/stats1.htm

بستراجبورغ –فرنسا– و التي جاءت بفصلين الأول تضمن الأحكام العامة التي تبين الغرض الأساسي من هذا البروتوكول و الثاني تكفل ببيان هذه الجرائم المعلوماتية و حصرها في السلوكات التالية:

- نشر المواد التي تتعلق بالعنصرية و كراهية الأجانب عبر أنظمة الكمبيوتر.
- التهديد الذي تحركه دوافع التمييز العنصري و كراهية الأجانب.
- الإهانة التي تحركها دوافع التمييز العنصري و كراهية الأجانب.
- الانكار أو التقليل أو الموافقة أو تبرير جرائم الإبادة الجماعية و جرائم ضد الإنسانية.

وهي الصور المجرمة نفسها تقريبا التي جاءت بها الفقرة 04 من المادة 15 من الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتية، و لكن نجدها غائبة عن مفاهيم التشريع العقابي الجزائري الذي لا زال يصر على تطبيق النصوص التقليدية في شكل المادة 298 ق 06–23 و المادة 298 مكرر ق 01–09 قانون العقوبات.

إذن فجرائم الذم القدح و التحقير يمكن أن تستهدف شخصا معينا بذاته أو مجموعة من الأشخاص تجمع بينهم قواسم مشتركة دينية أو عقائدية أو عرقية، و ذلك من خلال الاستعانة و الاعتماد على تقنية المعلوماتية بشكل كامل على اعتبار أنها الوسيلة الأقدر على نشر هذه الأنواع من السلوكات بأسرع و أشمل طريقة.

الفقرة الثانية: جرائم التعدي على البيانات الشخصية.

تعد الحياة الخاصة قطعة أساسية من كيان الإنسان، لا يمكن انتزاعها منه، و إن احترامها يعد من المبادئ الدستورية الثابتة، بحيث يعد الدستور بأن لحياة المواطنين الخاصة حرمة يحميها القانون، فلكل شخص الحق في أن تظل أسرار حياته الخاصة محجوبة عن العلنية و مضمونة من تدخل الغير و استطلاعه.[1]

و تشكل الجريمة المعلوماتية مظهرا حديثا، يهدد بخطر محدق البيانات الشخصية للأفراد من عدة زوايا نوجزها فيما يلي:

[1] محمد حسين منصور – مرجع سابق – ص 373.

أولا: جمع البيانات و تخزينها على نحو غير مشروع: يتمثل فعل انتهاك الحق في الحياة الخاصة للأفراد، في عملية جمع و تخزين بيانات صحيحة عنهم، و لكن على نحو غير مشروع، و يستمد هذه الصفة غير المشروعة من الأساليب المستخدمة لأجل الحصول على هذه البيانات أو من حيث طبيعة هذه البيانات.

فأما من حيث الأساليب فقد يعتمد الجاني على أسلوب التقاط ارتجاجات الجدران و ترجمتها إلى عبارات و كلمات و ذلك بواسطة معدات خاصة تغذي الحاسوب المزود ببرنامج خاص لترجمة كل ذلك، أو من خلال اعتراض الرسائل الإلكترونية، أو اختراق النظام المعلوماتي للضحية.

أما من حيث طبيعة البيانات فان البيانات الاسمية الخاصة يجب أن يحظر جمعها و تخزينها و معالجتها داخل الحاسوب من قبل الغير، إضافة إلى المعلومات المتعلقة بالسجل القضائي التي لا يحق إلا للسلطة القضائية جمعها و تخزينها حفاظا على سمعة الأشخاص.[1]

وهي الجرائم المنصوص عليها في نصوص المواد 303 مكرر و 303 مكرر 01 من قانون العقوبات الجزائري.

ثانيا: إساءة استعمال البيانات و المعلومات الاسمية (انتحال الشخصية) .

ترتكز جريمة انتحال الشخصية على مبدأ التعدي على البيانات الاسمية للغير، من أجل التخفي و التهرب من المسؤولية، أي الإفلات من المتابعة الجزائية، أي هي استخدام بيانات شخصية للغير من أجل الوصول إلى هدف غير مشروع، يتمثل في جريمة تحقق الربح المادي لمقترفها، دون أن يكون هو المتابع بشأنها، و قد أشارت الإحصائيات السنوية لسنة 2009 أن حوالي 210,000 شخص في فرنسا قد وقعوا ضحايا هذا النوع من الإجرام عبر الأنترنت، و يقدر معدل نموها على مستوى الدول الغربية ب 40%، و تشكل هذه الجريمة جزءا من جرائم الاحتيال المعلوماتي، فالفرد أصبح معرضا أكثر من أي وقت مضى لمخاطر

[1] نهلا عبد القادر المومني – مرجع سابق – ص 173-174.

انتحال هويته من قبل الغير بسبب اعتماده المطلق أو شبه الدائم على تقنية المعلوماتية و شبكة الأنترنت خصوصا، ضف إلى ذلك أن وسائل التحقق من الشخصية عبر الأنترنت هي غير تلك المتبعة أمام الجهات الرسمية فاسم المستعمل و كلمة السر و العنوان المنطقي، و رقم البطاقة البنكية هي وسائل إثبات الهوية المعلوماتية و هي الأجدر بالحماية، مقارنة بالاسم و اللقب و الصورة، و قد عرفت هذه الجرائم انتشارا رهيبا في السنوات الأخيرة من خلال انتشار تقنية المعلوماتية و قد علق عليها الأستاذ (أوليفي إيتاني Olivier Iteanu) بالقول: "لقد دخلنا مرحلة الهوية المستعملة" أي أنها قابلة للاستبدال بمجرد استعمالها أول مرة.[1]

ثالثا: إفشاء الأسرار و البيانات و المعلومات الاسمية: إن هذا النوع من السلوكات الإجرامية، قد يكون نتيجة حتمية للجرائم السالف ذكرها، بأن البيانات الخاصة قد انتقلت من السر إلى العلانية، بمجرد تخزينها بعد تجميعها على نحو غير مشروع أو حتى بصفة مشروعة، و بالتالي فإنها تكون عرضة للاطلاع عليها من قبل عدد غير محدد العدد من الأشخاص في حال عرضها على شبكة الأنترنت أو على الأقل من قبل عدد محدد متمثل في الأشخاص العاملين في فضاء المعلوماتية.

الفرع الثالث: جرائم الاستغلال الجنسي للأطفال عبر الأنترنت.

لم يسبق للبشرية منذ أن وجدت أن عرفت تقاربا بين الأفراد و الحضارات كالذي تعرفه اليوم، من خلال توفر تقنية المعلوماتية و شبكة الأنترنت، هذه الأخيرة أصبحت تشكل مصدر خطر و تهديد لاعتبارات عدة تتمثل أساسا في أنها شبكة تواصل بدون حدود، و بدون مركز إدارة قانونية، مما أتاح لفئة من المستعملين استغلالها بشكل مخالف للهدف الأساسي من إنشائها و هو تبادل المعارف،فأصبحت الوسيلة الفضلى لارتكاب جرائمهم النابعة من ميولهم الإجرامي و غاياتهم الدنيا، من خلال نشرهم و تبادلهم نصوص و مقاطع فيديو تخص الاستغلال الجنسي للأطفال في شكل مواد إباحية طفولية (Pédopornographie)[2].

---

[1] Myriam Quéméner- Yves Charpenel – La cybercriminalité - op.cit -p 89-90.

[2] Sofia Belghiti – "Les mineurs et les infractions a l'internet "– Article publier sur la Revue marocaine de l'enfant et de la famille – Num 01-janvier 2010 – le royaume Marocain - p 49-50.

تعتبر هذه الجرائم نتاج نطاق عالمية الأنترنت الذي يتيح نشر الأعمال المخلة بالآداب العامة و الأخلاق، و التي يتباين مفهومها من بلد لآخر، فاستخدام التقنية المعلوماتية في نشر المواد الإباحية التي تستهدف شريحة البالغين، قد لا تستثني شريحة الأطفال الذين قد يكونوا عرضة إما لهذه المواد الإباحية أو محلا لها مما يشكل اعتداءا ماديا و معنويا على الأطفال.[1]

و تشكل تقنية المعلوماتية تهديدا على فئة القصر و الأطفال من ثلاث 03 نواحي:

1- إمكانية ولوج الأطفال إلى مضمون المواقع الإباحية أو المواقع التي تظم دعارة الأطفال.

2- تخليد الانتهاكات الجنسية ضد الأطفال من خلال نشر هذه المواد على شبكة الأنترنت.

3- تشكل شبكة الأنترنت مرتعا للأشخاص الخطيرين المنجذبين لفئة الأطفال، و بالتالي فانه يمكن الإيقاع بهم.[2]

و مما يزيد من مخاطر الأنترنت على الأطفال هو اعتبارهم الفئة الأكثر انجذابا لهذه التقنية، و الأكثر تصفحا للإنترنيت فقد قدمت وكالة كاليستو لاتحاد صوت الطفل- Calysto pour la fédération de la voix de l'enfant إحصائيات تفيد بأن 12% من هذه الفئة تقضي أكثر من 03 ساعات يوميا في تفقد الرسائل الإلكترونية، و أن أكثر من 87% منهم قد تفاجأوا بمضامين اغرائية فاضحة، و بالتالي فان الأطفال هم الفريسة الأسهل على شبكة الأنترنت.[3]

إذا كان هذا هو واقع الحال و الذي ينذر بالخطورة، فماهي يا ترى الطبيعة القانونية لهذه الجرائم و إلى أي مدى يمتد نطاق الحماية القانونية لهذه الفئة في مواجهة هذه السلوكات الإجرامية بالذات؟

---

[1] تشير الإحصائيات في فرنسا إلى تنامي هذا النوع من الجرائم بحيث قفزت من 277 جريمة سنة 2009 إلى 362 جريمة سنة 2012- أنظر في ذلك: تقرير مجموعة العمل الحكومية المشتركة الفرنسية 2014- مرجع سابق- ص 20.

[2] محمد أمين الشوابكة – مرجع سابق – ص 106-107.

[3] Myriam Quéméner- Yves Charpenel – La cybercriminalité - op.cit – p 103.

الفقرة الأولى: مظاهر الحماية القانونية للأطفال عبر الأنترنت.

ظهرت المساعي الأولى لمكافحة الاستغلال الجنسي للأطفال عام 1999 بمناسبة مؤتمر فينا لمكافحة الاستغلال الجنسي للأطفال، و قد نصت المادة "34" من اتفاقية حقوق الطفل على أن يتعهد الأطراف على حماية الطفل من جميع أشكال الاستغلال الجنسي و الانتهاك الجنسي و ذلك من خلال اتخاذ جميع التدابير الوطنية و الثنائية و الجماعية الأطراف لمنع:

- حمل أو إكراه الطفل على تعاطي نشاط جنسي غير مشروع.
- الاستخدام الاستغلالي للأطفال في الدعارة.
- الاستخدام الاستغلالي للأطفال في العروض و المواد الداعرة...

وتأكيدا لذلك أقرت الجمعية العامة للأمم المتحدة بموجب المادة 01 من البروتوكول الاختياري لاتفاقية حقوق الطفل الصادر بموجب القرار رقم 263 المؤرخ في 25 ماي 2000 الداخل حيز التنفيذ في 18 جانفي 2002. بالقول بأنه: "يجب على الدول الأطراف حضر بيع الأطفال و استغلالهم في البغاء و المواد الإباحية"، و قد حددت المادة 03 الفقرة "ج" من نفس البروتوكول أن المقصود بالإباحية بقولها "يقصد باستغلال الأطفال في المواد الإباحية: تصوير أي طفل بأي وسيلة كانت، يمارس ممارسة حقيقية أو بالمحاكاة أنشطة صريحة أو أي تصوير للأعضاء التناسلية للطفل لإشباع الرغبة الجنسية أساسا.

أما على المستوى الإقليمي فنجد أن اتفاقية بودابست لسنة 2001 قد أفردت في نص مادتها التاسعة (09) مجموعة من الأحكام تلتزم بها الدول الموقعة تحت عنوان: الجرائم المتصلة بالمواد الإباحية للأطفال و التي جرمت السلوكات التالية:

- إنتاج مواد إباحية طفولية بغرض نشرها على نظام معلوماتي.
- تقديم أو إتاحة مادة إباحية طفولية عبر نظام معلوماتي.
- التزود أو تزويد الغير بمادة إباحية طفولية عبر نظام معلوماتي.

- حيازة مادة إباحية طفولية في نظام معلوماتي أو أية وسيلة تخزين.

و هي نفس التوصيات التي قدمتها الاتفاقية العربية لمواجهة جرائم تقنية المعلومات في نص الفقرة 02 و 03 من نص المادة 12 عشرا الموسومة بجريمة الإباحية ضد الأطفال.

أما على مستوى التشريعات الداخلية فيجب الإشارة إلى ما قدمه الفقه و التشريع الأمريكي تجاه جرائم الاستغلال الجنسي للأطفال باعتباره نموذجا للتشريعات الأنجلوساكسونية، بحيث يعتبر قانون آداب الاتصالات (CDA) الصادر عن الكونغرس الأمريكي سنة 1996، أول تشريع يجرم نقل المواد الإباحية الطفولية على شبكة الأنترنت من خلال ما نصت عليه المادة "18" منه و التي عرفت العرض الإباحي للمواد الطفولية بأنه كل تصوير مرئي يتضمن صورة أو فيلم أو فيديو، أو رسما أو رسم كمبيوتر أو صورة منتجة بطريق الكمبيوتر أو بوسيلة إلكترونية أو ميكانيكية أو بأي وسيلة كانت.

أما على مستوى التشريع الفرنسي فان نصوص المواد 227-01 و 02 و 227-23 تنصان على عقاب كل شخص قام بإغراء قاصر دون سن 15عشرا سنة بإغراءات ذات طابع جنسي باستعمال وسيلة اتصال إلكترونية بالحبس 02 سنتين و بغرامة قدرها 30,000 أورو، أو تشدد العقوبة إلى خمس 05 سنوات و غرامة قدرها 175,000 أورو في حالة ما إذا تمت المقابلة، و هي نفس العقوبة المقررة في حق كل من يسجل أو ينقل صورة لطفل بقصد نشرها إذا كانت إباحية و تشدد العقوبة إلى ما مقداره 10 سنوات سجنا و غرامة 100,000 أورو في حال نشرها و إتاحتها على شبكات الاتصال.

أما على مستوى التشريع الجزائري فتجريم هذا النوع من السلوكات جاء متأخرا جدا و ذلك بموجب القانون 14-04 المؤرخ في 04 فيفري **2014** الذي إستحدث نص المادة 333 مكرر1 ضمن قانون العقوبات الجزائري و التي جاء فيها" بأنه يعاقب بالحبس من 05 سنوات إلى 10 سنوات و بغرامة من 500 ألف إلى 1 مليون دج كل من صور قاصرا لم يكمل سن 18 سنة بأي وسيلة كانت و هو يمارس أنشطة جنسية بصفة

مبينة ،حقيقية أو غير حقيقية ، أو صور الأعضاء الجنسية للقاصر جنسية أساسا، أو قام بإنتاج أو توزيع أو نشر أو ترويج أو إستيراد أو تصدير أو عرض أو بيع او حيازة مواد إباحية متعلقة بالقصر.

في حال الإدانة تأمر الجهة القضائية بمصادرة الوسائل المستعملة لأرتكاب الجريمة و الأموال المتحصل عليها مع مراعاة حقوق الغير حسن النية" ، و بذلك فقد وسع المشرع من مظاهر الحماية الجزائية التي كانت محصورة في النصوص التقليدية كنص المادة 333 مكرر من قانون العقوبات و المواد 335 ق العقوبات المتعلقة بفعل المخل بالحياء و نصوص المواد من 342 إلى 349 المتعلقة بجريمة البغاء و جرائم التحرش الجنسي المقررة حسب نص م 341 مكرر من قانون العقوبات، و ذلك مسايرة منه للنسق الدولي التشريعي في مجال حماية الأطفال ضد مخاطر تكنولوجيا المعلومات ، غير ان النص لا يخلو من القصور فقد سهى المشرع عن تجريم فعل الإغراء عبر شبكات الإتصال ، و ركز مجال التجريم في أفعال التصوير و تصميم الصور الخاصة بالممارسة الجنسية، و نشرها و حيازتها، و لذلك و جب علينا تنبيه المشرع إلى هذا السهو و ضرورة إعادة صياغة النص و فق ما تفرضه الجريمة المعلوماتية من واقع و ليس ما يفرضه التصور القانوني فقط.

الفقرة الثانية: صور الاستغلال الجنسي للأطفال عبر الأنترنت.

إذا كان واقع الحال من الناحية التشريعية هو توحد الرؤى و النظرة تجاه ظاهرة الاستغلال الجنسي للأطفال عبر الأنترنت فان المظاهر المادية لهذه الظاهرة في اتساع و تزايد مستمر و يمكن حصرها تحت أوصاف عامة في شكلين أساسيين هما:

أولا: جريمة إغراء الأطفال عبر الأنترنت لغرض اباحي: تتحقق هذه الجريمة حسب ما أورده المشرع الفرنسي في نص المادة 227-22-1 من قانون العقوبات، لقيام الجاني بربط الاتصال مع الأطفال بغرض إغوائهم جنسيا و يكون الربط بواسطة إلكترونية و الغرض منها هو عقد لقاء معهم يقوم على هدف المعاشرة الجنسية يشارك فيها الطفل، و يتحقق ركنها المعنوي من خلال إلمام الجاني بعنصري العلم و الإرادة فيعلم أن سلوكه

محظور و أن الضحية قاصر و تتجه إرادته إلى الإغواء بهدف إشباع رغبته الجنسية، كما قد يكون الغرض أو السلوك مقتصرا على عرض مشاهد إباحية على الطفل.[1]

و هي الصورة الإجرامية التي تغيب على نصوص قانون العقوبات الجزائري بالرغم من تعديله مؤخرا ، و هي من أكثر السلوكات الشائعة و التي تستهدف فئة الأطفال.

ثانيا: جريمة استغلال صورة الطفل عبر الأنترنت في مواد إباحية: تتحقق هذه الجريمة وفق قانون العقوبات الجزائري نص المادة 333مكرر01 ق 14-04 تقابلها نص المادة 227-23 قانون عقوبات فرنسي ، من خلال ركنها المادي القائم على التقاط صور أو تصوير صور لطفل أو حيازتها أو نشرها أو تخزينها أو تزويد الغير بها لغرض إباحي، و يكون ذلك باستعمال الحاسوب و شبكة الاتصال،سواء كانت حقيقة أو مصطنعة، كما يتحقق ركنها المعنوي من خلال توفر القصد الجنائي أي علم الجاني بخطورة فعله و اتجاه إرادته إلى تحقيق هذه الحيازة أو الشر أو الإنتاج للمواد التي تستغل فيها صورة الطفل في أعمال إباحية.

إن ما يمكن استخلاصه في هذا الصدد هو أن جرائم التعدي على الأطفال من خلال المعلوماتية، تتمثل خصوصا في جرائم الاستغلال الجنسي la pédophilie، و التي يمكن أن تتعداها لصورة أخطر و هي جرائم الإباحية للأطفال la pédo pornographie الهدف منها إشباع الرغبات الدنيئة لفئة معينة من مستعملي شبكة المعلومات، يكون فيها الضحية الأول و الأخير هو الطفل الذي مازال لم يبلغ سن التمييز الذي يمكنه من إدراك حجم الضرر الذي لحق به، و في سبيل ذلك شددت اتفاقية الأمم المتحدة الأمريكية المتعلقة بحقوق الطفل على ضرورة تجاوز العقابات التشريعية في سبيل مواجهة هذا النوع من الجرائم و لعل أن أهمها هو ضرورة تحديد عمر افتراضي للطفل المشمول بالحماية على اعتبار أن اختلاف سن التمييز بين الدول يعتبر عائقا حقيقيا يقف في وجه توحيد الجهود الدولية لأجل القضاء على هذه الظاهرة اللاإنسانية.

[1] محمد أمين الشوابكة – مرجع سابق – ص 130.

خلاصة الفصل .

لم تعد تكنولوجيا المعلوماتية بمثابة تلك التقنية المحتكرة من قبل فئة الدول المتقدمة دون سواها ، و لا حكرا على مجتمعات دون الأخرى ، بل أصبحت منذ فترة السبعينيات من القرن الماضي و في العشرية الأخيرة خصوصا من التقنيات التي تشكل أحدى أساسيات الحياة للدول و المجتمعات الحديثة ، فقد إنتشرت على كافة المستويات و الأصعدة و الجوانب الحياتية ، فأصبحت الحواسيب و شبكة الأنترنت من الأمور المتصور أن يمتلكها بداهة كل فرد ، و تستعين بها كل هيئة و مؤسسة ، و هو ما ساعد على تطور الفكر البشري و كذلك نمط الحياة البشرية ، غير أن هذه التقنية ولدت خطرا و تهديدا على أمن و سلامة الدول و الأفراد ، من خلال السلوكات الإجرامية التي تعرف بالجرائم المعلوماتية ، أو بجرائم المساس بأنظمة المعالجة الآلية للمعلومات أو جرائم التقنية العالية ، و هي تلك الجرائم المنصوص عليها قانونا و التي تستهدف النظم المعلوماتية (الحواسيب و الشبكات) ، بغرض الإعتداء على أمن و سلامة وسرية المعلومات المتداولة عبرها أو المخزنة عليها ، و هي التي تتمتع بالحماية القانونية ، هذه الأخيرة أصبحت الهدف الرئيسي لفئة جديدة من المجرمين لم تكن معروفة من قبل و هم فئى مجرمي المعلوماتية ، فئة يميزها الذكاء و المعرفة الواسعة بمجال التكنولوجيا المعلوماتية ، و هو ما يستغلونه في مجال الإجرام المعلوماتي من خلال إبتكار و تنفيذ ما يعرف بالهجمات الإلكترونية ، هذه الإعتداءات التي تتسم بطابع السرية و الطابع المعنوي الخالص ، بالنظر إلى الوسائل و الأساليب الإلكترونية المعتمدة في تنفيذها ، كل ذلك إما بغرض الإطلاع على معلومات سرية و إما سرقتها أو تخريبها أو تعطيل عمل الأنظمة كليا ، كما قد يسعون إلى من خلال ذلك إلى تحقيق رغبات خاصة كالربح المادي أو الإعتداء على الغير ، بمن فيهم فئة القصر و الأطفال من خلال إستدراجهم عبر شبكة الأنترنت لغايات نفسية دنيئة تصل درجة الإستغلال الجنسي ، و هي الجرائم التي وضع لها القانون الجزائي إطارا تشريعيا و قانونيا مهما و ذلك بغرض مجابهة هذه الظاهرة الإجرامية بشكل لفعال .

و كخلاصة لما جاء في هذا الفصل يمكننا إيجاز بعض النتائج المتوصل إليها من خلال العرض الوارد في المبحثين السابقين و هي :

- أن التقنية المعلوماتية قد أصبحت من أساسيات الحياة في المجتمعات الحديثة بالرغم من فارق الإمكانات و مدى تفاوت معدلات الإنتشار بين الدول ، فأصبحت غالبية الدول حول العالم تعتمد على تقنية المعلوماتية ، و النظم المعلوماتية في تسير شؤونها و التعامل مع أفراد مجتمعاتها ، و هو نفس الحال بالنسبة للأفراد الذين أصبحت هذه التقنية جزءا لا يتجزأ من حياتهم اليومية.
- تجاوب الأنظمة التشريعية بشكل كبير مع التقنية المعلوماتية ، و من حيث شقها السلبي و ذلك من خلال وضع مجموعة من النصوص العقابية الموجهة إلى محاربة الجريمة المعلوماتية ، بهدف الحفاظ على الغاية الأول للتقنية المعلوماتية ألا و هي تسهيل تداول المعلومات و التعامل معها من اجل تسير أمور الدول و الحكومات ، و ضمان التواصل بين الشعوب و المجتمعات في ظل التبادل الإجتماعي و الفكري و ترقية الفكر البشري، و هو ما إتبعه المشرع الجزائري من خلال محاولة تأطيره لهذا المجال من خلال جملة النصوص التشريعية التي مست بالتعديل قانون العقوبات و قانون الإجراءات الجزائية ، و التي عمل من خلالها على خلق مركز قانوني مستقل للتقنية المعلوماتية ، من خلال تجريم السلوكات السلبية الناشئة عن سوء إستغلال هذه التقنية ، و كذلك وضع مجموعة من النصوص الإجرائية التي تضمن شرعية و فعالية مجموعة الإجراءات المتخذة في مواجهة مجرمي المعلوماتية ، و ذلك في شكل القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال.
- طغيان الجانب الإجرامي على التقنية المعلوماتية بشكل كبير، مما يتسسب في إعاقة المصالح العامة والخاصة لمستعمليها ، خصوصا و إتساع نطاق شبكة الأنترنت من يوم لأخر ، تزامنا و ظهور تقنيات حديثة للإتصال البيني بالشبكة من خلال تقنيات الهواتف الذكية و شبكات الإتصال اللاسلكية، فتعددت الجرائم بين ما يمس منها بأمن وسلامة النظم المعلوماتية ذاتها ، و بين ما يمس بأمن المعلومات المتداولة عبرها ، و بين ما

يستهدف الأشخاص سواء الإعتبارية منها كالدول و الحكومات و كبرى المؤسسات بهدف تحصيل معلومات مشمولة بطابع السرية ، أو الأشخاص الطبيعية بهدف إلحاق الضرر بهم ماديا من خلال سرقة حسابتهم البنكية و المالية ، أو معنويا من خلال التشهير بهم و الإنقاص من قيمتهم من خلال نشر أسرارهم أو التحريض على كراهيتهم ، و لعل أن الجرائم المتعلقة بالأشخاص و التي تتصدر قائمة الجرائم الأشد خطورة تبقى تلك الجرائم التي تستهدف الأطفال عبر الشبكات و التي تهدف إلى الإيقاع بهم تحت قبضة الشواذ جنسيا ، نظرا لضعف إدراكهم بحجم الضرر الذي يستهدفهم.

- ظهور فئة جديدة من المجرمين هم " مجرمي المعلوماتية " الذين لا يقلون خطورة عن غيرهم ، بالرغم من عدم لجوؤهم إلى مظاهر العنف المادي أثناء تنفيذ جرائمهم ، و ذلك نظرا لخطورتهم الكامنة وراء ذكائهم و خبرتهم في مجال المعلوماتية ، و شغفهم و إصرارهم على تحدي كافة الوسائل الموضوعة لحماية المعلومات و النظم المعلوماتية ، و صعوبة الكشف عن هويتهم بالنظر إلى طابعهم الإجتماعي غالبا و قدراتهم العلمية ، و التي تبدد الشكوك من حولهم غالبا.
- ظهور مجموعة من الإشكاليات الحديثة متعلقة بالجانب الإجرائي في مواجهة الجريمة المعلوماتية بالنظر إلى طابعها اللامادي ، و عدم ملائمة النصوص الإجرائية التقليدية في التعامل و هذا النوع المستحدث من الجرائم ، و هو ما سيكون موضوع دراستنا في الفصل الموالي.

الفصل الثاني

مسألة شرعية إجراءات البحث و التحقيق في الجرائم المعلوماتية و الجهات المختصة بتنفيذها

لطالما كانت الجرائم محل متابعة و بحث و تحقيق، و ذلك تحقيقا للغرض الأول و هو الكشف عن هوية مرتكبها و تقديمه للعدالة من أجل أن ينال الجزاء المقرر ، عقابا له على فعله و اقتصاصا منه للضحية و المجتمع ، و هو ما أصبح يعرف حديثا حسب نظرية " الردع الجزائي" بتحقيق الردع العام و الخاص ، فلم يتدخل الفقه و لا القضاء يوما من أجل تحديد قائمة الجرائم التي يجوز أن تكون تحت مجهر الإجراءات الجزائية ، من تلك الأخرى التي لا يجوز تفعيل هذه الإجراءات بشأنها ، فكل الجرائم كانت و لا زالت و من حيث طبيعتها على قدم المساواة أمام فصول القوانين الإجرائية ، و ذلك نظرا لطابعها المادي المشترك ، غير أن ظهور الجريمة المعلوماتية المرتبطة بإستعمال تكنولوجيات حديثة ذات طابع معنوي يخلو من المظاهر المادية ، خلق نوعا من الإرتباك تمثل في إنقسام رأي الفقه و القانون حول مدى قابلية و شرعية مباشرة إجراءات ذات طابع جزائي مادي في مواجهة جريمة ذات طابع معنوي ، سعيا وراء دليل لا يمكن ضبطه بالوسائل المعتادة في الجرائم التقليدية ، و ذلك بسبب عدم ملائمة النصوص الإجرائية التقليدية لهذا النوع الحديث من الجرائم ، و إعاقتها للسير الحسن لأعمال البحث و التحقيق نتيجة عدم تناسبها و إياها، كما كانت الجرائم المعلوماتية سببا مباشرا في ظهور عقبات جدية في عمل الجهات المنوط بها أعمال البحث و التحقيق في الجرائم العادية ، فالجرائم المعلوماتية تحتاج إلى خبرات فنية و علمية و أخرى قانونية ، و قدرات ذهنية خاصة ، و محققا من نوع خاص له من التكوين في المجال و التخصص، ما يسمح له بإكتساب نفسية مختلفة تتوافق و تفكير مجرمي المعلوماتية ، لآجل التصرف مع هذه الجرائم بالشكل المطلوب، و ذلك نظرا لسرعة تنفيذها و طابعها الخفي و القدرة على تدمير أدلتها في وقت قياسي ، و هي العقبات التي جعلت القائمين على عمل جهات البحث و التحقيق امام حل و حيد و هو ضرورة تشكيل فرق خاصة تتولى أمر متابعة جرائم و مجرمي المعلوماتية دون غيرهم ، إن كل هذه الإشكاليات لم تكن تخطر على بال و فكر فقهاء القانون و لا المشرعين و لا على القائمين على جهات

تنفيذ القانون ، غير انه و في ظل الواقع الرقمي الذي أضحى يسيطر على حياة المجتمعات و الشعوب ، و في ظل تنامي الظاهرة الإجرامية المعلوماتية و تزايد حدة خطورتها و تهديدها للأمن العام و الخاص ، أصبح الكل منشغلا بإيجاد الحلول الفقهية منها و التشريعية و تجسيدها من خلال طرحها عمليا على الجهات المختصة لأجل مجابهة الجريمة المعلوماتية ، و يمكن إيجاز كل تلك الإنشغالات في مضمون الإشكالية الفرعية التالية : إلى إي مدى تكيف الفقه و القانون مع الظاهرة الإجرامية المعلوماتية ؟ و إلى أي مدى ساهم كل ذلك في تطوير آليات عمل جهات البحث و التحقيق ؟

إن الإجابة عن كل ذلك إستدعت منا إتباع خطة فرعية خاصة بهذا الفصل تتضح من خلال مبحثين رئيسين هما :

المبحث الأول الموسوم بـ: النظم المعلوماتية وإجراءات البحث و التحقيق بين رأي الفقه و أحكام القانون، و ذلك على مختلف المستويات الدولية و الإقليمية و الداخلية، و الذي نعالج من خلاله الأثر الفقهي و القانوني الذي خلفته الجريمة المعلوماتية ، خصوصا من حيث شرعية الإجراءات الجزائية المتخذة في مواجهتها.

المبحث الثاني و الذي إخترنا له عنوانا أوجزناه في : الهيئات المختصة بمهام البحث و التحقيق في الجرائم المعلوماتية ، و ذلك على شتى المستويات الدولية منها و الإقليمية و الوطنية .

المبحث الأول: النظم المعلوماتية وإجراءات البحث و التحقيق بين رأي الفقه و أحكام القانون.

لطالما اعتبرت النظم المعلوماتية (الحواسيب و الشبكات) في نهاية القرن الماضي ثروة مكتسبة للدول الغربية المتقدمة دون غيرها من الدول الأخرى نظرا لتحكمها التام في مجالات تصنيعها واستخدامها، غير أن هذه التقنية وفي ظل الوقت الراهن أصبحت في متناول الكل وعلى أدنى المستويات الاجتماعية وهو ما خلق نوعا جديدا من السلوكات السلبية المتصلة باستعمال هذه التكنولوجيا في صورة الجريمة المعلوماتية كما سبق وأن فصلنا سابقا.[1]

إن الجريمة المعلوماتية بوصفها نوعا مستحدثا على أحكام قانون العقوبات و القوانين الإجرائية الجزائية، شكلت عنصرا جدلياً بين الفقه و القانون فيما يتعلق بمبدأ أحقيتها بمكانة خاصة في المنظومة القانونية العقابية منها و الإجرائية ،غير أن واقع الحال المتمثل في مدى خطورتها وحجم خسائرها جعل من أمر هذا النقاش أمرا محسوما بفضل الحماية القانونية التي توفرها الأنظمة التشريعية لهذه التقنية باعتبارها من أساسيات الحياة اليومية للمجتمعات و عمل أجهزة الدول و الحكومات، إن هذا التحول المحتوم في مسار التشريعات العقابية و الإجرائية من التقليدي المادي إلى المستحدث الرقمي،لم يكن بالسلاسة المعتادة وذلك بفعل الطبيعة الخاصة للجرائم المعلوماتية التي تعتمد أساليب ووسائل خاصة وتنتج عنها دلائل من نوع خاص، وكلها معطيات يستلزم أن يكون تحت مجهر رجال البحث و التحقيق في مجال متابعة مرتكبيها، فتكييف التشريع مع هذا النوع من الجرائم لازال لم يستقر بعد على موقف موحد بفعل التغيرات التي تطرأ على هذا النوع من الجرائم بفعل خاصيتها المتمثلة في التطور الدائم و المستمر، فقد ثارت

---

[1] – من مجموع عدد سكان القارة الإفريقية المقدر بـ: 1,125,664,947 مليار نسمة حسب تقديرات شهر جانفي 2014، فإن ما مجموعه 205,185,547 مليون نسمة يستعملون شبكة الأنترنت أي بمعدل إنتشار يقدر بـ: 18 % ، و هو معدل إنتشار ضعيف مقارنة بالأوروبي المقدر بـ : 78% أو الأمريكي الشمالي المقدر بـ: 81 % .

أنظر في ذلك : The Global Digital Statistic 2014– op cit – p23 .

ولازالت تثار إشكاليات جديدة أمام رجال البحث و التحقيق الجنائي أمام معطيات الجريمة المعلوماتية تجعل منهم أحيانا عاجزين عن أداء مهامهم بصفة عادية وقد يطال البطلان جملة إجراءاتهم بفعل تناقضها مع أحكام التشريع الخاصة بهذا النوع من الجرائم، و الإشكالية التي تثار في هذا الشأن هو إلى أي مدى يعترف الفقه و القانون بالطبيعة القانونية للنظم المعلوماتية من أجل اعتبارها محلا مشروعا لأعمال البحث والتحقيق الجنائي؟

إن الإجابة عن هذه الإشكالية الفرعية تستدعي منا مناقشة مدى قابلية النظم المعلوماتية لأن تكون محلا لأعمال البحث و التحقيق (المطلب الأول)، إضافة إلى الإشكالية المتعلقة بمسائل الاختصاص الإقليمي التي تواجه أعمال البحث و التحقيق(المطلب الثاني) ، لننطرق ختاما إلى مظاهر التعاون الدولي وأثرها على التشريعات الداخلية في مجال ترقية أعمال البحث و التحقيق الجنائي بما فيها التشريع الجزائري (المطلب الثالث).

المطلب الأول: مدى قابلية النظم المعلوماتية لأن تكون محل بحث وتحقيق جنائي .

تقتضي قواعد العدالة الجنائية، تحريك الدعوى العمومية ضد كل من تسول له نفسه مخالفة أحكام وقواعد قانون العقوبات بما في ذلك المجرم المعلوماتي ،وذلك بغرض عقابه جزاء له على فعله الإجرامي، إن مسائل المتابعة الجزائية في مجال الجرائم المعلوماتية تقتضي إتباع نوع خاص من الإجراءات التي يمكن وصفها بأنها أعمال التفتيش، و التي تتأثر حتما و وجوبا بطبيعة موضوعها كالنظم المعلوماتية (الفرع الأول)، و التي تستهدف بالبحث و التحقيق المكونات الخاصة بالنظم المعلوماتية المادية منها ، و المعنوية (الفرع الثاني) أو قد يكون محلها الشبكات المتصلة بها ، (الفرع الثالث) ، و قبل التعرض إلى مسائل الجدل القائم حول مدى قابلية النظم المعلوماتية لأن تكون محلا للتفتيش وجب علينا طرح التساؤل التالي: هل هناك فرق بين تفتيش الأشخاص و الأماكن، وتفتيش النظم المعلوماتية؟

الفرع الأول : أثر طبيعة النظم المعلوماتية على أعمال التفتيش .

لم تتضمن التشريعات العربية على اختلافها تعريفا قانونيا للتفتيش كإجراء بما فيها التشريع الجزائري، ولكن الفقه العربي أورد تعريفات متعددة للتفتيش كإجراء تحقيقي، فقد عرفه بأنه الإطلاع على محل له حرمة للبحث عما يفيد التحقيق، تقوم به السلطة التي حددها القانون، يتم بالبحث في مستودع السر عن أدلة الجريمة التي وقعت وكل ما يفيد في كشف الحقيقة، وتمثل مستودع السر في شخص المتهم، و المكان الذي يعمل به أو يقيم فيه، وعرف كذلك بأنه إجراء من إجراءات التحقيق التي تهدف إلى ضبط أدلة الجريمة موضوع التحقيق وكل ما يفيد في كشف الحقيقة[1].

يتضح من خلال استقرائنا للتعريف السابق أن التفتيش ما هو إلا وسيلة للإثبات المادي، لأنه يستهدف بحكم طبيعته الأشياء المادية المتعلقة بالجريمة أو التي تفيد في كشف الحقيقة، وغايته دوما هي الحصول على الدليل المادي، وهذا ما يتنافى مع الطبيعة المعنوية للبرامج و البيانات الحاسوبية وكذلك شبكة الانترنت و الشبكات الأخرى، فهي مجرد برامج وبيانات الكترونية ليس لها أي مظهر مادي محسوس، فلا سبيل أن يرد عليها تفتيش ومن الأجدر إخضاعها إلى أحكام مستقلة تتلائم وطبيعتها الخاصة ، ولذلك فقد نادى جانب من الفقه إلى وجوب إطلاق مصطلح خاص على عملية البحث و التحقيق بشأن الجريمة المعلوماتية كالولوج أو النفاد باعتباره المصطلح الملائم وطبيعة الجريمة[2].

---

[1]- علي حسن أحمد الطوالبة- التفتيش الجنائي على نظم الحاسوب و الانترنت- دراسة مقارنة- عالم الكتب الحديث – اربط- الأردن – 2004- ص 10.

[2]- نبيلة هبة هروال- الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الإستدلالات – دار الفكر الجامعي- الإسكندرية- مصر – 2007- ص 223.

وقد أثار تفتيش النظم المعلوماتية زيادة على مسألة التناقض في المصطلح، نقاشا حول طبيعته في مجال النظم المعلوماتية، هل هو إجراء خاص بمرحلة الإستدلال أم بمرحلة التحقيق فقط؟ وقد انقسم الفقه في ذلك إلى أربع طوائف مختلفة يتخذ كل منها حججا خاصة في تبريره لطبيعة هذا الإجراء.

الفقرة الأولى : أنصار الاتجاه الأول.

يأخذ أنصار هذا الاتجاه في تحديدهم لطبيعة التفتيش القانونية في مجال الجرائم المعلوماتية بالهدف المتوخى منه، وبحسبهم فإن الغاية من التفتيش هي الحصول على الأدلة وضبطها وكشف حقيقتها وإزالة الغموض بشأنها ونسبها إلى شخص معين، وهي نفس الغاية التي تهدف إلى ضبط المعطيات غير المشروعة من الحاسوب الخاص بالمتهم وتقديمها كدليل ضده أمام المحكمة.

الفقرة الثانية : أنصار الاتجاه الثاني.

يرى أصحابه أن التفتيش كإجراء تتحدد طبيعته حسب المرحلة التي تكون فيها الدعوى الجزائية، فإذا ما تم قبل تحريكها، فهو عمل من أعمال البحث و الاستدلال، أما إذا ما تم بعد ذلك فإنه عمل من أعمال التحقيق، وهو المعيار الذي لا يمكن تطبيقه بسهولة نظرا لطبيعة الجريمة المعلوماتية فقد تضطر سلطة التحقيق إلى القيام ببعض أعمال التحري كالتصنت و التجسس المعلوماتي وهو ما يجعل من أمر تحديد طبيعة هذا الإجراء أمرا صعبا[1].

الفقرة الثالثة: أنصار الاتجاه الثالث.

يستند أصحاب هذا المذهب في تحديد طبيعة التفتيش إلى صفة القائم به، فإن قام به أحد أعضاء التحقيق فهو عمل من أعمال التحقيق أما إن قام به أعضاء وضباط الشرطة القضائية فإنه يعد عمل من أعمال البحث و الاستدلال.

---

[1]– علي حسن أحمد الطوالبة–التفتيش الجنائي على نظم الحاسوب و الانترنت– دراسة مقارنة –مرجع سابق– ص 15.

الفقرة الرابعة : أنصار الاتجاه الرابع.

وهو اتجاه مختلط حاول التوفيق بين الاتجاهات السابقة وبحسبهم فإن الطبيعة القانونية للتفتيش تستند إلى القول بأن هذا الأخير يعد من إجراءات التحقيق إذا ما قامت به السلطة المختصة بالتحقيق وبعد تحريك الدعوى العمومية ومباشرتها بقصد الكشف عن الحقيقة ، أي أنه عمل من اعمال الإستدلال إذا ما قامت به السلطة المختصة بالبحث و قبل تحريك الدعوى العمومية [1].

و من جهتنا و كرأي خاص فإننا نؤيد رأي الفقه الرابع الذي يعتبر التفتيش عملا ذو طبيعة مزدوجة فهو من اعمال البحث إذا ما باشرته السلطات المختصة بالبحث و التحري قبل تحريك الدعوى، و من أعمال التحقيق إذا ما تمت مباشرته بقصد الوصول إلى الحقيقة من قبل السلطة المختصة بذلك بعد تحريك الدعوى ، فلا يمكن تصنيفه ضمن أعمال التحقيق فقط ،لأنه و في مجال الجرائم المعلوماتية يمكن إتخاذ إجراءات خاصة بالتحقيق أثناء مرحلة الإستدلال ، كالوضع تحت المراقبة الإلكترونية ، كما أن القائم بالتحقيق له ان ينيب ضباط الشرطة القضائية للقيام بأعمال التحقيق بدلا عنه .

إذن فاعتبار التفتيش إجراءأ قانونيا شرعيا، وجب علينا التساؤل عن مدى نطاق تطبيقه ، هل هو إجراء يستهدف المكونات المادية للنظم المعلوماتية فقط؟ أم يمتد إلى باقي المكونات المنطقية للنظم المعلوماتية ؟

الفرع الثاني : مدى قابلية المكونات المادية للحاسوب لأن تكون محلا للتفتيش.

يعتبر الحاسوب من أهم مكونات النظم المعلوماتية باعتباره أداة التحكم الآلي في المعطيات بما فيها تلك الموجهة لإرتكاب الجريمة وهو ما يجعل منه مستودع سر المجرم المعلوماتي، ومجال أعمال البحث و التحقيق الجنائيين فإلى أي مدى يمكن أن تنطبق قواعد التفتيش على مكونات الحواسيب المادية منها و المنطقية؟

---

[1]– علي حسن أحمد الطوالبة– التفتيش الجنائي على نظم الحاسوب و الانترنت– دراسة مقارنة– مرجع سابق– ص 16.

لا يختلف اثنان في أن الولوج إلى المكونات المادية للحاسوب (Hard ware) بحثا عن شيء ما يتصل بجريمة معلوماتية وقعت قد يفيد في كشف الحقيقة عنها وعن مرتكبها، يخضع للإجراءات القانونية التقليدية الخاصة بالتفتيش، بمعنى أن تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه هل هو من الأماكن العامة أو الخاصة ، فلطبيعة المكان أهمية قصوى خاصة في مجال التفتيش، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكم، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه بنفس الضمانات المقررة قانونا في التشريعات المختلفة[1].

ففي القانون الجزائري لا يجوز القيام بهذا الإجراء إلا بعد حصول على إذن مكتوب من السلطة المختصة (وكيل الجمهورية / قاضي التحقيق) إضافة إلى رضا صريح من صاحب ذلك المسكن مكتوب وموقع بخط يده و إن ثبت بأن صاحب السكن لا يعرف الكتابة ينوه عن ذلك في المحضر أما إن تعذر عليه الحضور فإن ضابط الشرطة القضائية المكلف بإتمام الإجراء ملزم بأن يعين ممثلا له، وإذا ما امتنع أو كان هاربا، استدعى الضابط لإتمام ذلك شاهدين من غير الموظفين الخاضعين لسلطة كما يجب أن يتم الإجراء حسب المواعيد الزمنية المقررة لذلك[2].

غير أن الإجراء وفي مجال الجرائم المعلوماتية يحظى بدعم تشريعي أكبر بحيث تنص كل من المادة 45 قانون 06-22 من قانون الإجراءات الجزائية في فقرتها الأخيرة أنه و بالنسبة للجرائم المعلوماتية فإنه لا مجال لتطبيق الضمانات المقررة لعمليات التفتيش المقررة سالفا، عدا ما تعلق منها بإستظهار الإذن و الحفاظ على السر المهني و جرد الأشياء المحجوزة، بالإضافة إلى ما تقرره المادة 47 فقرة 03 قانون 06- 22 من نفس القانون على أنه إذا ما تعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود

[1]- علي عدنان الفيل – إجراءات التحري و جمع الأدلة و التحقيق الإبتدائي في الجريمة المعلوماتية- دراسة مقارنة- دار الكتاب الجامعي الحديث- الإسكندرية- مصر - 2012- ص 41.

[2]- المواد 45-47 ق 06-22 من قانون الإجراءات الجزائية الجزائري.

الوطنية أو الجرائم الماسة بأنظمة الحاسب فإنه يجوز إجراء التفتيش و المعاينة و الحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار و الليل بناء على إذن مسبب من وكيل الجمهورية المختص.

أما بالنسبة للأماكن العمومية (العامة)، فإذا ما وجد الشخص وهو يحمل مكونات الحاسوب المادية أو كان مسيطرا عليها أو حائزا لها، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات و القيود المخصصة لهذا الصدد.

ومن التطبيقات التشريعية التي تجيز تفتيش مكونات الحاسوب ما تخوله بعض التشريعات الإجرائية لسلطات التحقيق في سبيل اتخاذ أي إجراء أو شيء لازم لجمع الأدلة، ما تنص عليه المادة 251 من قانون الإجراءات الجزائية اليوناني و المادة 487 من القانون الجنائي الكندي، إضافة إلى تشريع لوكسمبورغ و الولايات المتحدة الأمريكية[1].

ويمكن القول بأن أغلب التشريعات القانونية قد استندت إلى مبدأ جواز التعامل وفق قواعد التفتيش مع المكونات المادية للحاسوب طالما أنها ذات طبيعة مادية محسوسة، ومفيدة في كشف الحقيقة و وفقا لذلك نص المشرع الجزائري في نص المادة 30 الفقرة 01 من المرسوم الرئاسي رقم 15-261 المتعلق بتحديد و تنظيم و كيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها الصادر بتاريخ 08 أكتوبر 2015 و المنشور بالجريدة الرسمية رقم : 53 لنفس السنة بالقول " يمكن ان يقوم القضاة و ضباط الشرطة القضائية التابعون للهيئة أثناء تأديتهم لوظائفهم أو بمناسبتها طبقا للشروط و الكيفيات المنصوص عليها في التشريع الساري المفعول و لا سيما لقانون الإجراءات الجزائية بتفتيش إي هيكل او جهاز بلغ إلى علمهم أنه يحوز أو يستعمل وسائل و تجهيزات موجهة لمراقبة

[1]- نزيهة مكاري-" وسائل الإثبات في جرائم الاعتداء على حق المؤلف عبر الانترنت"- مقالة علمية منشورة بمجلة المناهج القانونية- العدد المزدوج 13-14 - سنة 2009- دون ذكر المعلومات المتعلقة بهيئة النشر-المملكة المغربية- ص 59.

الإتصالات الإلكترونية" إن صدور هذا النص يعتبر تصريحا وضحا عن نية المشرع في تخصيص نصوص إجرائية ذات طبيعة خاصة و متوافقة مع طبيعة الجرائم المعلوماتية و عناصرها ، فالنصوص المقررة سابقا في ظل القانون الإجرائي او القانون 09-04 المتعلق بالوقاية من الجرائم المعلوماتية، لم تشر أي منها إلى إتاحة التفتيش المادي الموجه إلى المكونات المادية للنظم المعلوماتية ، كالحواسيب و الأجهزة المستعملة في إرتكاب الجريمة و إعتبرتها من قبيل الأشياء المادية القابلة للتفتيش بحسب أحكام النصوص الإجرائية العادية ، إذن فهذا التغيير في النهج التشريعي يعبر و بصراحة عن رأي المشرع الجزائري في إتاحة تفتيش المكونات المادية المتصلة بالجرائم المعلوماتية.

الفرع الثالث : مدى خضوع المكونات المنطقية للحاسوب للتفتيش.

لقد أثارت مسألة خضوع المكونات المنطقية للحاسوب (البرامج و البيانات) لإجراءات التفتيش، أو الولوج في إطار إجراءات البحث و التحقيق الجنائي جدلا فقهيا بين اتجاهين أساسيين في هذا المجال بين مؤيد ومعارض لمسألة جواز اعتبار المكونات المنطقية للحاسوب محلا للإجراءات التفتيش.

الفقرة الأولى : الاتجاه المعارض لإمكانية خضوع مكونات الحاسوب المنطقية للتفتيش.

يتمثل فكر هذا الاتجاه في عدم إمكانية انسجام وتطابق أحكام التفتيش و الضبط في القانون الجنائي الإجرائي مع ما قد يتطلبه كشف الحقيقة في الجرائم المعلوماتية من بحث وتفتيش عن الأدلة في برامج الحاسوب وبياناته[1].

---

[1]- علي حسن أحمد الطوالبة- التفتيش الجنائي على نظم الحاسوب و الانترنت - دراسة مقارنة- مرجع سابق- ص 30.

فأصحابه يرون أنه لا يمكن تصور إجراء التفتيش على الكيانات المنطقية لانتفاء الكيان المادي عنها، ويرى فقهاء هذا الاتجاه أن برامج وبيانات الحاسوب ليست مثل الأشياء المادية المحسوسة و بالتالي لا يقع الضبط عليها[1].

فهناك من التشريعات الإجرائية التي حددت هدف التفتيش في البحث عن الشيء (Objet) أو أشياء وضبطها، وهذا الشيء ينطبق بمفهومه على المال ذي الحيز المادي المحسوس ولا يمتد إلى الكيانات المنطقية ، أي البرامج و البيانات و التطبيقات غير المحسوسة فالأصل في الأشياء أن تكون مادية ذات حيز مادي محسوس، و القانون لم يعرف قبلا الأشياء غير المادية إلا من خلال التقدم البشري و التطور التكنولوجي الذي صاحبه ظهور قيم جديدة غير مادية[2].

ومن التشريعات التي أخذت بهذا المبدأ التشريع الفرنسي الذي يرى فقهاؤه أن النبضات و الإشارات الالكترونية الممغنطة لا تعد من قبل الأشياء المحسوسة وبالتالي لا تعتبر شيئا ماديا، وهو ما أدى بالمشرع لتعديل النصوص بموجب القانون 545-2004- المؤرخ في 21-06 - 2004 بإضافة عبارة "المعطيات المعلوماتية" لنص المادة 94 من قانون الإجراءات الجزائية[3].

الفقرة الثانية : الاتجاه المؤيد لخضوع الكيانات المنطقية للحاسوب للتفتيش.

يرى أصحاب هذا الرأي بجواز ضبط البيانات الإلكترونية من خلال خضوعها لإجراءات التفتيش و يستمد هؤلاء رأيهم إلى أن القوانين الإجرائية عندما تنص على إصدار الإذن بضبط أي (شيء) ، فإن

---

[1]- علي حسن أحمد الطوالبة-"إجراءات ضبط المكونات المعنوية للحاسوب و الانترنت"- بحث منشور على الموقع الإلكتروني لمركز الإعلام الأمني- أكاديمية الشرطة البحرينية- مملكة البحرين- أفريل 2011- ص 3- تاريخ التصفح: 2014/05/29- الرابط الإلكتروني:

http://www.policemc.gov.bh/reports/2011/April/30-4- 2011/634397721383881294.pdf

[2]- علي حسن أحمد الطوالبة- التفتيش الجنائي على نظم الحاسوب و الانترنت- دراسة مقارنة -مرجع سابق ص 31.

[3]-عائشة بن قارة- حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري و القانون المقارن- دار الجامعة الجديدة – الإسكندرية – مصر - 2010 – ص 91.

ذلك يجب تفسيره بحيث يشمل بيانات الحاسوب المادية و المنطقية ،لأن الغاية من التفتيش هي ضبط الأدلة التي تفيد في كشف الحقيقة وبذلك يمتد المفهوم ليشمل البيانات الإلكترونية بمختلف أشكالها (برامج – تطبيقات– بيانات)[1].

ويميز أصحاب هذا الاتجاه بين المعلومات و البيانات المعالجة آليا ،فينفون الطابع المادي عن الأولى ويؤكدونه للثانية، على أساس أنها ذبذبات إلكترونية وإشارات وموجات كهرومغناطيسية قابلة لأن تسجل وتخزن على وسائط مادية، وبالتالي فهم ينفون عن هذه البيانات الطابع المعنوي مؤكدين بأنها شيء يمكن لمسه في المحيط الخارجي و أنها كيان مادي لا يمكن إنكاره مستندين في ذلك إلى حكم محكمة الجنح ببروكسل (بلجيكا) الذي أكد على كون هذه البيانات أشياء مادية محسوسة.[2]

كما يستند هؤلاء على مبدأ أن البرامج و البيانات تشغل حيزا ماديا في ذاكرة الحاسوب ويمكن قياس حجمها بالبايت (byte) و الكيلوبايت (k.b) و الميغابايت وهكذا تحدد حجم الذاكرة الداخلية للحاسوب.[3]

ويعتبر الفقه الكندي من أمثلة الفقه الذي توسع في تفسير نصوص القانون الإجرائي لكي يتوافق مع هذا الرأي، فحسب نص المادة 487 من قانون العقوبات الكندي يمكن إصدار أمر قضائي لتفتيش وضبط أي شيء تتوفر أسس أو مبررات معقولة تدعو للاعتقاد بأن جريمة ما قد وقعت، أو يشتبه في وقوعها أو أن هناك نية لاستخدامه في ارتكاب جريمة مستقبلا[4].

و في نفس الإطار يفسر الفقه اليوناني عبارة أي شيء، بأنها تشمل بالضبط البيانات المخزنة أو المعالجة إلكترونيا، ولذلك فإن ضبط البيانات المخزنة في الذاكرة الداخلية للحاسوب لا يشكل أي مشكلة

---

[1]– علي عدنان الفيل– مرجع سابق– ص 42.

[2]– علي حسن أحمد الطوالبة–"إجراءات ضبط المكونات المعنوية للحاسوب و الانترنت"– مرجع سابق ص 04.

[3]– علي حسن أحمد الطوالبة– التفتيش الجنائي على نظم الحاسوب و الانترنت– دراسة مقارنة – مرجع سابق ص 32.

[4]– فتوح الشادلي – عفيفي كامل عفيفي – جرائم الكمبيوتر وحقوق المؤلف و المصنفات الفنية ودور الشرطة– منشورات الحلبي الحقوقية– بيروت – لبنان– دون ذكر سنة النشر– ص 366.

في اليونان، فبمقدور المحقق أن يعطي أمرا للخبير بجمع البيانات التي يمكن أن تكون مقبولة كدليل في المحاكمة الجنائية وذلك حسب المادة 251 من قانون الإجراءات الجزائية اليوناني[1].

إذن فمن الواضح جليا أن التشريعات قد تأقلمت مع الواقع الحديث و التكنولوجي للجريمة المعلوماتية من خلال إقرار قوانين ذات طابع عام يتماشى وكل حالات التفتيش بما فيها الواقعة على المكونات المعنوية منها و المادية للحاسوب، أو من خلال إقرار نصوص تشريعية ذات طابع خاص موجهة لمسائل التفتيش التي يكون محلها الحاسوب المنطقية خصوصا.

وهو ما حذى عليه المشرع الجزائري بموجب نص المادة 05 و 06 من القانون 04-09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال بالقول في نص المادة 05 الفقرة الأولى :" يجوز للسلطات القضائية المختصة و كذا ضباط الشرطة القضائية ، في إطار قانون الإجراءات الجزائية و في الحالات المنصوص عليها في المادة 04 الدخول بغرض التفتيش و لو عن بعد إلى : منظومة معلوماتية أو جزء منها و كذا المعطيات المخزنة فيها و كذلك إلى منظومة تخزين معلوماتية" ، كما جاء في نص المادة 06 من نفس القانون أنه " عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها و أنه ليس من الضروري حجز كل المنظومة ، يتم نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونة تكون قابلة للحجز و الوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية ، يجب في كل الأحوال على السلطة التي تقوم بالتفتيش و الحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.

---

[1]- عبد الله حسين علي محمود- "إجراءات جمع الأدلة في مجال سرقة المعلومات"- بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الإلكترونية – مركز البحوث و الدراسات- أكاديمية شرطة دبي- دبي- الإمارات العربية المتحدة- من 26 إلى 28 أفريل 2003- ص 05.

غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للإستغلال لأغراض التحقيق شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات".

و هو ما يوضح توجه المشرع الجزائري إلى إتاحة التعامل مع المكونات المنطقية للحاسوب وفق إجراءات البحث و التحقيق الجنائي ، من خلال إخضاعها لأعمال التفتيش حسب القواعد الخاصة المقررة لذلك .

المطلب الثاني: مدى قابلية الشبكات للتفتيش (التفتيش عن بعد).

كما سبق و أن عرفنا وبينا مفهوم الشبكة في نطاق النظام المعلوماتي لا بأس بأن نذكر بأن شبكة الحاسوب (Network) هي تلك المجموعة المكونة من اثنين أو أكثر من أجهزة الحاسوب المتصلة بعضها البعض اتصالا سلكيا أو لا سلكيا ، قد تكون محلية LAN أو واسعة النطاق WAN أو دولية انترنت[1].

وكما سبق و أن فصلنا أن عمل هذه الشبكات هو ضمان نقل المعلومات و البيانات بين أجهزة الحواسيب وتخزينها واسترجاعها في أي وقت ومن أي مكان يتصل منه المستخدم، وبالتالي فإن عمل الشبكات قد أصبح الوسيلة الأولى التي يستعين بها مجرمو المعلوماتية من أجل تنفيذ هجماتهم الالكترونية ضد ضحاياهم وهو يفسر طابع الدولية الذي يميز الجريمة المعلوماتية عن غيرها من الجرائم، إن أثار هذه الجرائم قد تكون مخزنة عبر الشبكة أو على ذاكرة حاسوبية أو قاعدة بيانات لدولة أجنبية منتقلة من مكان لآخر وهو ما يجعل من أمر إخضاعها لأعمال البحث و التحقيق أي للتفتيش أمرا محتوما و ضروريا، وذلك بهدف إحراز الدليل الذي يفيد في كشف الحقيقة ونسبها إلى فاعلها، و إن كان أمر إخضاع المكونات المنطقية للحاسوب قد أصبح وفي نظرنا جائزا و لا تثير إشكالا من حيث خضوع هذه المكونات لقانون العقوبات و القوانين الإجرائية بالرغم من طابعها المعنوي، فإن ما يمكن إثارته من إشكال هو مسائل الاختصاص الإقليمي التي يثيرها أمر إخضاع هذه البيانات للتفتيش عبر الشبكة نظرا للطابع الدولي لشبكة

[1]– علي حسن أحمد الطوالبة– التفتيش الجنائي على نظم الحاسوب و الانترنت– دراسة مقارنة– مرجع سابق– ص 34.

الاتصالات الدولية "الانترنت" و التي تعتبر السبيل و الوسيلة الفضلى لمجرمي المعلوماتية في مجال تنفيذ أعمالهم الإجرامية؟ ولذلك سنحاول الإجابة على هذه الإشكالية و التعرض لمسألة تفتيش الشبكة البينية بين جهازي حاسوب المتهم و حاسوب أخر داخل نفس الإقليم (الفرع الأول) وتلك المتصلة بينهما داخل إقليم دولتين مختلفتين (الفرع الثاني) لنختم كل ذلك بمدى شرعية تفتيش المرسلات الالكترونية (الفرع الثالث).

الفرع الأول: تفتيش الشبكة البينية الرابطة بين جهاز حاسوب المتهم وحاسوب أخر داخل نفس الإقليم.

يمكن أن يكون جهاز حاسوب المتهم موضوع إجراءات التفتيش متصلا من خلال الشبكة بجهاز حاسوب آخر داخل نفس الدولة التي وقعت بها الجريمة المعلوماتية ،فهل يجوز أن يمتد التفتيش عبر الشبكة إلى الحاسوب الآخر الذي قد يحوز أدلة مفيدة في كشف الحقيقة، ذلك قبل وصول الجاني إليها ومحوها بفعل شرط استصدار أمر بالتفتيش كما هو الحال بالنسبة لحاسوب المتهم؟

إن الإجابة عن هذه الإشكالية كانت محل اهتمام فقهي الذي رأى بشأنها أنه يجب توسيع سلطات الجهة المعنية بمباشرة عملية التفتيش وذلك من خلال منحها حق ولوج النظم المعلوماتية المتصلة بحاسوب المتهم دون شرط الحصول على إذن من السلطة المختصة، إذا كان من شأن انتظار صدور الإذن أن يفوت فرصة الحصول على الدليل.

وقد تبنت بعض التشريعات المقارنة هذا الاتجاه ومنها قانون تحقيق الجنايات البلجيكي الصادر في 23-11-2000 الذي يجيز مد التفتيش إلى نظام معلوماتي آخر غير ذلك الموجود في مكان مباشرة الإجراء الأصلي وذلك تحت ظروف الضرورة الحتمية لكشف الحقيقة بخصوص الجريمة، أو أن تكون الأدلة معرضة لخطر الإتلاف، وهو ما أقرته الاتفاقية الأوروبية لبودابست لمكافحة الجرائم المعلوماتية في نص المادة "19" .[1]

---

[1] – للإطلاع على نص المادة كاملا راجع نص الإتفاقية .

أما في الولايات المتحدة الأمريكية فإن المادة (A/41) من قانون الإجراءات الجنائية الفيدرالية الأمريكي ، منحت لقاضي التحقيق إصدار إذن تفتيش ملكية داخل منطقة أو خارجها، متى كانت الملكية عند طلب الإذن موجودة داخل المنطقة ولكن يخشى أو يتوقع تحركها خارجها قبل تنفيذ الإذن[1].

وهو ما نجده أيضا في القانون الاتحادي الأسترالي حيث لم تعد صلاحيات التفتيش المختصة بالجرائم المعلوماتية مقتصرة على مواقع محددة فحسب، فبموجب قانون جرائم الانترنت لعام 2001 أصبح يسمح بمد عمليات التفتيش عن البيانات خارج المواقع التي يمكن اختراقها، من خلال حواسيب توجد في الأبنية الجاري تفتيشها ويشير مصطلح " البيانات المحتجزة في حاسبة ما" إلى ما مفهومه أنه بيانات محتجزة في جهاز تخزين على شبكة ربط بين الحواسيب فلا توجد حدود جغرافية محددة و لا أي شرط بالحصول على موافقة طرف ثالث[2].

كما نصت بدورها المادة 17 فقرة (أ) من القانون الفرنسي رقم 239 لسنة 2003 للأمن الداخلي الصادر في 18-03-2003 بأنه يمكن لرجال الضبط القضائي أن يدخلوا من الجهاز الرئيسي إلى البيانات التي تهم عملية البحث و التحري ، فتنص بذلك بأنه يجوز لرجال الضبط القضائي من درجة الضباط وغيرهم من رجال الضبط القضائي، أن يدخلوا عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي يتم التفتيش على البيانات التي تهم التحقيق، و المخزنة في النظام المذكور أو في أي نظام معلوماتي آخر مادامت هذه البيانات متصلة في شبكة واحدة مع النظام الرئيسي أو تم الدخول إليها أو تكون متاحة ابتداء من النظام الرئيسي[3].

---

[1]– موسى مسعود أرحومة– الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية– بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية و القانون – 28،29 أكتوبر 2009– أكاديمية الدراسات العليا– طرابلس – ليبيا– ص 10.

[2]– علي عدنان الفيل – مرجع سابق– ص 45.

[3]– نزيهة مكاري – مرجع سابق –ص 61.

أما على مستوى التشريع الجزائري فإنه و حسب ما تنص عليه الفقرة 02 من نص المادة 05 من القانون 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها، فإنه يمكن للسلطات القضائية المختصة و كذلك لضباط الشرطة القضائية و مراعاة لأحكام قانون الإجراءات الجزائية ، الدخول بغرض التفتيش عن بعد لكل منظومة معلوماتية و بسرعة ، إذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة عليها ، و أنه يمكن الدخول إليها إنطلاقا من المنظومة الأولى ، و ذلك بشرط إعلام السلطة القضائية المختصة مسبقا، و بالتالي فإنه يجوز مد التفتيش داخل الإقليم من منظومة معلوماتية إلى أخرى بدون أي إشكال متى توفر داعي الإعتقاد بأن المعلومات محل البحث مخزنة على تلك المنظومة بشرط وحيد و هو إعلام السلطة القضائية المختصة .

ويشترط على كل حال أن يكون الغرض من إجراء هذا التفتيش صادقا وغايته التوصل إلى أدلة تتعلق بالجريمة التي يجري بشأنها التحقيق أو ما يفيد في كشف الحقيقة عنها وعن مرتكبيها، فلا يجوز مباشرته إلا إذا كان هدفه واضحا من البداية، أما إذا كان الهدف منه هو الإطلاع غير المصرح به على ملفات البيانات المخزنة داخل نظام الحاسوب لإحدى المؤسسات أو الشركات أو الغير فيعتبر الإجراء باطلا ويشكل في حد ذاته جريمة معلوماتية عبر شبكة الانترنت[1].

وعلى العكس من ذلك فهناك من التشريعات المقارنة التي تقصر إذن التفتيش على الأجهزة الموجودة في مكان محدد دون امتدادها إلى الأجهزة الأخرى المرتبطة بها كما هو عليه الحالي في التشريع السويسري[2].

---

[1]- علي حسن أحمد الطوالبة- التفتيش الجنائي على نظم الحاسوب و الانترنت- دراسة مقارنة -مرجع سابق- ص 44.

[2]- عائشة بن قارة- مرجع سابق- ص 95.

الفرع الثاني : في حال اتصال حاسوب المتهم بآخر خارج إقليم الدولة.

من الإشكاليات التي تواجه سلطات البحث و التحقيق في مجال جمع الأدلة الالكترونية بشأن الجرائم المعلوماتية، و التي عرضها الأستاذ: سيبر أولريتش SIEBER–ULRICH ، قيام مرتكبي الجرائم المعلوماتية بتخزين بياناتهم في أنظمة معلوماتية خارج نطاق الدولة عن طريق شبكة الانترنت بهدف عرقلة التحقيقات.[1]

فهل يجوز متابعة إجراءات البحث و التحقيق خارج نطاق الإختصاص القضائي الإقليمي؟

الفقرة الأولى : الإتجاه الفقهي المعارض لمسألة جواز مد التفتيش عن بعد .

لقد تباينت الاتجاهات الفقهية حول مدى جواز امتداد التفتيش للحواسب المتصلة بحاسوب المتهم الواقعة خارج الدولة، فذهب رأي إلى رفض امتداد التفتيش لهذه الحواسيب، بدعوى أن ذلك ينطوي على انتهاك لسيادة دولة أخرى وهو ما يشكل اعتداءا على ولاية الدولة التي يجري التفتيش في نطاق إقليمها ومن ثم فإن الأمر يتطلب اللجوء إلى إجراءات طلب المساعدة القضائية أو الإنابة القضائية من السلطات الموازية في الدولة الأخرى، وبعبارة أخرى فإن مباشرة هذا الإجراء سيستلزم وجود اتفاقية تعاون قضائي ثنائية أو متعددة الأطراف و إلا فقد الإجراء مشروعيته، ولأجل مواجهة ذلك وضع الفقه الهولندي حلا يتمثل في طلب إلتماس من قبل سلطات الدولة الطالبة إلى الدولة الموجودة على إقليمها البيانات المخزنة لأجل منحها إيها و إرسالها، وهو إجراء يتعارض ومبدأ شرعية التحقيق في هذا النوع من الجرائم، وبناء على ذلك فلا إمتداد للتفتيش دوليا إلا بموجب اتفاقية دولية وهو الرأي السائد في الفقه الألماني، وتبعا لذلك فقد عرضت على القضاء الألماني واقعة غش معلوماتي محلها طرفي الحاسوب أحدهما بألمانيا و الآخر بسويسرا ولم يتم استرجاع البيانات المخزنة بالخارج إلا من خلال إلتماس المساعدة المتبادلة.[2]

---

[1]– نبيلة هبة هروال – مرجع سابق– ص 240.

[2]– موسى مسعود أرحومة – مرجع سابق – ص 11.

ومع ذلك فقد أجازت المادة 32 من الاتفاقية الأوروبية لبودابست إمكانية الدخول بغرض التفتيش و الضبط في أجهزة وشبكات معلوماتية تابعة لدول أخرى من دون إذنها في حالتين : إذا كانت المعلومات المخزنة في قاعدة بيانات متاحة للجمهور، أو إذا رضى صاحب أو حائز هذه البيانات بهذا التفتيش، غير أن تطبيق هذا النص يمكن أن يثير مشاكل عدة جراء تمسك كل دولة بمبادئ سيادتها، وهو ما يجعل من أمر الاتفاقيات الدولية الثنائية أو المتعددة الأطراف أمرا لامناص منه[1].

الفقرة الثانية : الفقة المؤيد لمد التفتيش عن بعد للنظم المعلوماتية.

بالمقابل من ذلك أيد جانب آخر من الفقه أمر امتداد التفتيش إلى الحواسيب الموجودة خارج إقليم الدولة وهو رأي يستند إلى مبررات واقعية، فمعتنقوه يحاولون التعامل مع واقع الصعوبات التي تعترض سلطات التحقيق وهو الاتجاه الذي أخذ به القانون الفرنسي حسب ما جاء في الفقرة 02 من المادة 17 من قانون الأمن الداخلي رقم 239 لسنة 2003 بإجازة تفتيش الأنظمة المعلوماتية المتصلة بحاسوب المتهم من قبل مأموري الضبط القضائي حتى ولو تواجدت خارج الإقليم شرط أن يراعى في ذلك الشروط المنصوص عليها في المعاهدات الدولية، وهو ما يسمح به كذلك قانون التحقيق الجنائي البلجيكي حسب نص مادته 88 التي تجيز لقاضي التحقيق الحصول على نسخة من البيانات التي هو بحاجة إليها دون انتظار إذن من سلطات الدولة الأخرى، ويبرر الفقه في فرنسا وبلجيكا ذلك بأن العالم الافتراضي لا يعرف الحدود.

أما في الولايات المتحدة الأمريكية فإن الأمر متعلق بوضع القائم بالتفتيش ،فإذا كان هذا الأخير يعلم قبل مباشرته البحث عن البيانات المخزنة بأنها تقع بعيدا و في نطاق إقليم دولة أخرى، فإنه يجب أن يقدم طلب التماس مساعدة إلى السلطات الدولة الأخرى، أما إذا كان يجهل ذلك أو لم يكن في وسعه معرفة ذلك

---

[1]- علي عدنان الفيل- مرجع سابق- ص 47.

فإن ما يسفر عنه التفتيش لا يهدر ويمكن قبوله و الركون إليه في الإثبات بوصفه دليلا ما اطمأنت إليه المحكمة ، فوفق القانون الأمريكي فإن رجال الضبط و التحقيق ملزمون بالتقييد بمبدأ ضرورة الإعلان عن وجودهم و الإفصاح عن ذلك أمام السلطات الأجنبية وهو ما يعرف بمبدأ الاستئذان و الإعلان، غير أنه يجوز لهم في نفس الوقت التحلل من هذه القاعدة متى راودهم شك بأن الالتزام بهذا المبدأ من شأنه إعاقة أعمال البحث و التحقيق التي باشروها وذلك حسب ما قضت به المحكمة الفيدرالية الأمريكية العليا[1].

الفقرة الثالثة: موقف المشرع الجزائري من مسألة التفتيش عن بعد.

بين الرأيين المؤيد و الرافض لفكرة جواز مد التفتيش عن بعد عبر الشبكات للأنظمة المعلوماتية،في مجال مباشرة أعمال البحث و التحقيق بشأن الجرائم المعلوماتية، اختار المشرع الجزائري الرأي المعارض لمسألة تمديد التفتيش دون إذن من السلطات الأجنبية فقد جاء في الفصل الثالث، تحت عنوان القواعد الإجرائية الخاصة بتفتيش المنظومات المعلوماتية من القانون 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و في الفقرة 03 من نص المادة 05 على أنه: " إذا تبين مسبقا بأن المعطيات المبحوث عنها و التي يمكن الدخول إليها إنطلاقا من المنظومة الأولى ، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني ، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة و وفقا لمبدأ المعاملة بالمثل ".

وبذلك فقد اختار المشرع الجزائري وفي هذا المجال السبيل الأطول إجرائيا نظرا لطول مدة إعداد و إرسال واستقبال الطلبات وطبيعة ونوع البيانات المراد تحصيلها، مقارنة بسرعة الجناة في مجال محو وتدمير الأدلة، و ذلك بالرغم مما ورد في نص المادتين 16 و 17 من نفس القانون و اللتان أقرتا بجملة من الأحكام العملية في مجال المساعدة القضائية الدولية المتبادلة بالقول بأنه : و في إطار التحريات

---

[1]- موسى مسعود أرحومة – مرجع سابق – ص 11- 12.

و التحقيقات القضائية الجارية لمعاينة الجرائم المعلوماتية، و كشف أمر مرتكبيها ، فإنه يمكن للسلطات المختصة و في إطار المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة، إرسال و إستقبال الطلبات الخاصة بذلك بالشكل الإلكتروني ، كأجهزة الفاكس و البريد الإلكتروني ، بشرط التأكد من مدى قدرتها على توفير الحماية و الأمن الكافي للمعلومات المرسلة و المستقبلة ، و كل ذلك وفقا للإتفاقيات الدولية و مبدأ المعاملة بالمثل ، و يمكن للسلطات الجزائرية في هذا الخصوص حسب نص المادة 18 من نفس القانون ، رفض تقديم المساعدة إذا كانت الطلبات الواردة بشأن ذلك من شأنها المساس بالسيادة الوطنية و النظام العام ، و للسلطات المختصة تقييد تقديم المساعدة بشرط الحفاظ على سرية المعلومات المقدمة ، و عدم إستعمالها خارج نطاق موضع الطلب ، وهو ما يشكل عائقا إجرائيا يقف في وجه السير الحسن لإجراءات البحث و التحقيق في الجرائم المعلوماتية ، بسبب الوقت المستغرق لأجل لإتمام الإجراءات حتى و لو كانت إلكترونية ، فلا حبذ لو اقتدى المشرع بنظيره من التشريع الأمريكي في هذا المجال، خصوصا دعم حصانة رجال البحث و التحقيق في مواجهة طائلة البطلان الإجرائي، من خلال تخويلهم سلطة تقديرية واسعة في مجال تقرير سير أعمال البحث و التحقيق التي يكلفون بها.[1]

الفرع الثالث: مشروعية تفتيش وضبط المراسلات الالكترونية (التصنت الالكتروني).

يتمتع صاحب البريد الإلكتروني بالحق في حرية الحياة الخاصة، بالنسبة لبريده الإلكتروني ومحتوياته، و تقيم أحكام القضاء التماثل بين مراسلات البريد الإلكتروني و المراسلات التي تتم عن طريق

---

[1]– زيادة على قواعد الإختصاص المنصوص عليها في قانون الإجراءات الجزائية ، تختص الجهات القضائية الجزائرية بالنظر في الجرائم المعلوماتية التي تقع خارج الإقليم الوطني ، أي في الخارج و ذلك إذا كان مرتكبها أجنبيا و إستهدف بفعله مؤسسات الدولة الجزائرية أو مصالح الدفاع الوطني ، او المصالح الإستراتيجية للإقتصاد الوطني نص المادة 15 قانون 09–04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال.

البريد العادي،فلا يجوز التدخل للإطلاع على البريد الإلكتروني للشخص دون إذنه ما لم يصدر إذن قضائي بذلك[1].

الفقرة الأولى : الضمانات التشريعية لمبدأ سرية المراسلات .

تجسد هذا المبدأ في مختلف النصوص القانونية على اختلاف درجاتها فنجده منصوصا عليه في نص المادة 12 من الإعلان العالمي لحقوق الإنسان الذي أُعتمد ونشر على الملأ بموجب قرار الجمعية العامة للأمم المتحدة 217 –ألف (د–3) المؤرخ في 10 ديسمبر 1948 " لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات".

كما تنص المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية الذي أُعتمد من قبل الجمعية العامة للأمم في 16 ديسمبر 1966 بأنه" لا يحوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته، من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس"، و هو ما تتفق بشأنه و توضحه نصوص المواد 08 من الاتفاقية الأوروبية لحقوق الإنسان لسنة 1950، و المادة 11 من الاتفاقية الأمريكية لحقوق الإنسان لسنة 1969 ، و كذلك المادة 21 من الميثاق العربي لحقوق الإنسان في نسخته الحديثة الذي أُعتمد من قبل القمة العربية السادسة عشرة التي استضافتها تونس في 23ماي 2004.

---

[1]– نزيهة مكاري– مرجع سابق– ص– 63.

أما على المستوى الوطني فنجد أن الدولة الجزائرية ملتزمة وفق أحكام الدستور بضمان حرمة الحياة الخاصة للمواطن، من خلال ضمان سرية المراسلات و الاتصالات الخاصة بكل أشكالها،بحيث تنص المادة 46 من دستور الجمهورية الديمقراطية الشعبية لسنة 1996 المعدل بموجب القانون رقم 16-01 المؤرخ في 06 مارس 2016 المنشور في الجريدة الرسمية رقم 14 المؤرخة في 7 مارس 2016 على أنه : " لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون ، سرّية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة ، لا يجوز بأي شكل المساس بهذه الحقوق دون امر معلل من السلطة القضائية، و يعاقب القانون على إنتهاك هذا الحكم، حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون و يعاقب على إنتهاكه" ، وقد واجهت في سبيل تحقيق ذلك كل موظف أو عون من أعوان الدولة أو مستخدم أو مندوب عن مصلحة البريد بعقوبة مقدارها الحبس من (03) ثلاث أشهر إلى (05) خمس سنوات وبغرامة من 30.000 إلى 50.000 دج في حال قام أي منهم بإتلاف رسائل بريدية أو تسهيل فضها أو اختلاسها أو إتلافها حسب ما تقضي به المادة 137- ق 06-23 من قانون العقوبات الجزائري، وهو ما أكدته المادة 127 الفقرة 01 و 02 و 03 من الفصل الثاني تحت عنوان الأحكام الجزائية الخاصة من القانون 2000-03 المؤرخ في 05 أوت 2000 المحدد للقواعد المتعلقة بالبريد و المواصلات السلكية و اللاسلكية بالقول: تطبق العقوبات المنصوص عليها في المادة 137- ق 06-23 من قانون العقوبات على ان كل شخص مرخص له بتقديم خدمة البريد السريع الدولي أو كل عون يعمل لديه و الذي في إطار ممارسة مهامه ، يفتح أو يحول أو يخرب البريد أو ينتهك سرية المراسلات أو يساعد في إرتكاب هذه الأفعال ، و تسري نفس العقوبات على كل شخص مرخص له بتقديم خدمة مواصلات سلكية و لا سلكية و على كل عامل لدى متعاملي الشبكات العمومية للمواصلات السلكية و اللاسلكية و الذي في إطار أداء مهامه ينتهك بأي طريقة كانت سرية المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق المواصلات السلكية و اللاسلكية ، أو الذي أمر أو ساعد في إرتكاب هذه الأفعال"

بالإضافة إلى الجزاءات التي تقررها نصوص المواد 303 إلى 303 مكرر ق 06-23 من نفس القانون بالنسبة للأشخاص العاديين، و التي تنص على انه كل من يفض أو يتلف رسائل أو مراسلات

موجهة للغير و ذلك بسوء نية و ذلك في غير الحالات المنصوص عليها في المادة 137 يعلقب بالحبس من شهر واحد إلى سنة و بغرامة من 25000 دج إلى 100,000 دج أو بإحدى هاتين العقوبتين.[1]

أما إذا ما تعمد أياً كان المساس بحرمه الحياة الشخصية للأشخاص بإستعمال أساليب تقنية كإلتقاط أو تسجيل أو نقل مكالمات او أحاديث خاصة أو سرية ، أو صور لشخص في مكان خاص ، بغير إذن صاحبها او شرع في ذلك فإن العقوبة تكون من 06 ستة أشهر إلى 03 ثلاث سنوات حبسا و بغرامة من 50,000دج إلى 300,000دج ، و تطبق نفس العقوبة على كل من إحتفظ أو وضع أو سمح بوضع في متناول الجمهور او الغير و بأي وسيلة كانت التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة الأفعال السابقة.[2]

إن كل هذه الضمانات المتعلقة بسرية وأمن المراسلات بما فيها السلكية و اللاسلكية أي الإلكترونية، و المعروفة تحت اسم – البريد الإلكتروني – راجعة أساسا إلى تشابه خدمة الرسائل العادية و الإلكترونية، بحيث أن البريد الإلكتروني يحتوي على برامج متخصصة لكتابة وإرسال و استقبال وعرض وتخزين الرسائل الإلكترونية، و من الخدمات التي تقدمها الرسائل ما يعرف بالتوقيع الإلكتروني، فبدل كتابة الاسم نهاية كل رسالة يقدم البرنامج إمضائه ومعلوماته، وعادة ما تكون الرسائل الإلكترونية محمية بكلمات سر وشفرات لا يمكن سوى للعارفين بها من الإطلاع عليها، و التعامل مع الرسائل الإلكترونية لا يختلف عن العادة فيمكن للمستخدم أن يقرئها ويرد عليها أو ينقلها للغير.[3]

و غالبا ما يكون البريد الإلكتروني وسيلة إجرامية يستعين بها المجرم المعلوماتي للإطاحة بضحاياه من خلال إتباع أسلوب الصيد الإلكتروني و الإغراق بالرسائل الإلكترونية أو الاحتيال كما سبق وأن بيناه

[1] – المادة 303 ق 06–23 قانون العقوبات الجزائري.

[2] – المادة 303 مكرر و المادة 303 مكرر 1 ق 06–23 قانون العقوبات الجزائري.

[3]– علي حسن أحمد الطوالبة– "إجراءات ضبط المكونات المعنوية للحاسوب و الانترنت" –مرجع سابق – ص 07.

مسبقا ولذلك كان من الواجب على رجال البحث و التحقيق أن يضعوا هذه الخدمة محل تفتيش وضبط باعتبارها أحد أهم مصادر الأدلة الإلكترونية غير أن عملهم ومهامهم ستصطدم مباشرة بجملة من العوائق في شكل ضمانات قانونية تضمن حرمة هذه المراسلات، وهو ما يطرح إشكالية مدى شرعية الإجراءات الجزائية المتخذة في مواجهة حرمة وسرية البريد الإلكتروني؟

الفقرة الثانية : مبدأ سرية المراسلات الإلكترونية و مكافحة الجرائم المعلوماتية.

تتباين ردود الأفعال التشريعية من مسألة جواز إنتهاك سرية المراسلات الإلكترونية في سبيل إتمام أعمال البحث و التحقيق في مجال الجرائم المعلوماتية، و قد إخترنا النموذجين الفرنسي و الجزائري للدراسة حسب ما هو وارد.

أولا : مسألة جواز إلتقاط المراسلات الإلكترونية في التشريع الفرنسي.

جاء في نص المادة 100 إلى 100-7 من قانون الإجراءات الجزائية الفرنسي على انه لقاضي التحقيق الأمر بالإلتقاط المراسلات عبر وسائل الاتصال عندما تفرض مقتضيات التحقيق في مواد الجنايات و الجنح ذلك، و إذا كانت العقوبة المقررة تساوي أو تزيد عن سنتين (02)، ويكون الأمر بالإلتقاط السري للمراسلات مكتوبا وجوبا ومسببا من قبل قاضي التحقيق وغير قابل لأي طعن لمدة (04) أربع أشهر قابلة للتمديد مرة واحدة.

يدخل حيز التنفيذ النظام القانوني الخاص بمسائل إلتقاط المراسلات بدءا من لحظة بداية التحقيقات و ذلك بشأن المراسلات الشخصية للأشخاص المتصلين بالشبكة، و ذلك من خلال تقنية خاصة تعمل من خلال تركيب جهاز اعتراض مغناطيسي على خط الشخص الموضوع محل المراقبة بهدف الحصول على عنوانه الإلكتروني (IP) ومن ثم الوصول إلى مكانه وتحديد هويته.[1]

[1]– Myriam Quéméner– Yves Charpenel – La Cybercriminalité – op.cit– p 174.

ثانيا : الإشكالية على مستوى التشريع الجزائري .

في سبيل تحقيق مصلحة المجتمع من خلال الاقتصاص من المجرم بما في ذلك المعلوماتي اهتدى المشرع الجزائري، إلى وضع نصوص تشريعية تتيح عمليات التصنت و المراقبة الإلكترونية على مراسلات المجرم المعلوماتي بكل أشكالها، وفي سبيل ذلك فقد نصت المادة 02 الفقرة "و" من القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال على وضع تعريف لمفهوم الاتصالات الإلكترونية ،بوصفها عمليات التراسل و الإرسال و الاستقبال لعلامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية .[1]، إضافة إلى ما جاء في نص المادة 03 من القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال على أنه " مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات و الإتصالات ، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية ،وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية و في هذا القانون ، وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية و تجميع و تسجيل محتواها في حينها ...." و هو الإجراء الذي تنظم أحكامه نص (المادة/04) من الفصل الثاني تحت عنوان مراقبة الاتصالات الإلكترونية من نفس القانون و التي تسمح باللجوء إلى المراقبة الإلكترونية من أجل الوقاية من الجرائم الإرهابية و التخريبية و الماسة منها بأمن الدولة ، أو من أجل المساعدة في التحقيقات القضائية الجارية سواء منها على المستوى الداخلي او الخارجي بناء

---

[1] يقصد بالإتصالات الإلكترونية حسب نص (المادة 05 فقرة 01) من المرسوم الرئاسي 15-261 الذي يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها" كل تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها عن طريق أي وسيلة إلكترونية بما في ذلك وسائل الهاتف الثابت و النقال " و قد أضاف نص هذه المادة وسيلتي الهاتف الثابت و النقال في إطار توسيع مجال أعمال البحث و التحقيق إلى كل جهاز يمكن ان يكون وسيلة في إرتكاب الجريمة.

على طلبات المساعدة القضائية الصادرة من الدول الأجنبية، و قد تدعم هذا الإجراء بموجب إنشاء هيئة وطنية لمكافحة الجرائم المعلوماتية بتاريخ 08 أكتوبر 2015 بموجب صدور المرسوم الرئاسي 261-15 و التي أصبحت تتولى و بصفة عملية إجراءات تنفيذ هذا الإجراء بمقتضى نصوص المواد من 21 إلى 26 منه ،و التي تبين طبيعة الترتيبات القانونية و التقنية الواجب مراعاتها تحقيقا لهذا الغرض ، و ضمانا لحرمة الحياة الخاصة للأفراد و سرية مراسلاتهم الإلكترونية ، من خلال اشتراطها لوجوب إستصدار رخصة قانونية مكتوبة صادرة عن السلطة القضائية و تولي هذه الأخيرة العملية لضان شرعية الإجراءات، بالإضافة إلى حصر اختصاص الهيئة بتنفيذ إجراء المراقبة الإلكترونية في نطاق الجرائم الموصوفة بأنها جرائم إرهابية او تخريبية او ماسة بأمن الدولة ، و ذلك تحت سلطة القاضي المختص مع حتمية الإلتزام بالحفاظ على سرية المعطيات المتحصل عليها و إستعمالها في النطاق المقرر لها دون سواه .

إذن فمن خلال استقراء وتحليل النصوص القانونية السالفة الذكر يتضح لنا نية المشرع الجزائري الدالة على جواز مراقبة الاتصالات الإلكترونية في مجمل الحالات بالرغم من طابعها الحصري، بما في ذلك البريد الإلكتروني أو المكالمات الهاتفية وذلك تيسيرا لأعمال البحث و التحقيق الجنائي في مجال الجرائم المعلوماتية.

إذن فمما سبق يتضح جليا أن القانون الإجرائي الجزائي و الفقه كذلك قد تأقلم مع طبيعة الجريمة المعلوماتية، بحيث وفر لها مناخا فقهيا و قانونيا ملائما يدعم أعمال البحث و التحقيق بشأنها، ولكن على مستويات مختلفة منها ما هو مسير ومنها ما معرقل لها أو غير متوافق مع الطابع الخاص للجريمة المعلوماتية، وفي خضم ذلك نستطيع أن نقول بأن التشريع الجزائري وفي هذا المجال يعتبر تشريعا فتيا نظرا لحداثة عهده مع هذه التقنيات، فهو لا زال يعاني قصورا من عديد النواحي و لعل أن البارز منها هو عدم تفريد نصوص إجرائية خاصة ضمن فصول القانون الإجرائي ، ضمانا لشرعية الإجراءات المتخذة

و تيسيرا لها ، و ذلك من خلال تجنب تداخل النصوص القانونية و ضمان عدم الإلتباس و تضييع الوقت في مباشرة الإجراءات التي يفترض في إتخاذها السرعة القصوى و الدقة لأجل الإحاطة بكل التفاصيل المتعلقة بالجريمة قبل طمسها و ضياعها .

المطلب الثالث: الجهود القانونية في سبيل دعم أعمال البحث و التحقيق في الجرائم المعلوماتية.

يمكن ارتكاب الجريمة المعلوماتية من أقصى نقطة بالأرض بنفس السهولة التي يمكن بها ارتكاب نفس الجريمة من أقرب مكان، فرسالة الإلكترونية واحدة يمكنها أن تكون وسيلة لارتكاب جريمة معلوماتية واحدة عبر عدة دول مختلفة لكل دولة منها نظام قانوني مختلف عن الآخر، مع الأخذ بعين الاعتبار بأن الأدلة و الآثار الرقمية التي يجب تتبعها لأجل تحديد هوية الجاني ومتابعته هي آثار سريعة الزوال مما يستوجب اتخاذ إجراءات ذات طابع سريع لأجل تحصيلها، غير أن بطء الإجراءات الرسمية قد يعرض نفس الأدلة للفقد، فقد تكون دول و بلدان عديدة ضحية نفس الجريمة المعلوماتية، مما يجعل من أمر تتبع وحفظ سلسلة الأدلة تحديا كبيرا، بل إن بعض الجرائم المعلوماتية المحلية قد يكون لها بعد دولي وربما تكون هناك الحاجة إلى طلب المساعدة من جميع البلدان التي مرت الجريمة من خلالها، فإذا دعت ضرورة التحقيق تفعيل الإجراءات في مواجهة الجريمة المعلوماتية فإن ذلك يستدعي بالضرورة مساعدة السلطات في البلد منشأ لجريمة وكذلك البلدان الضحايا وكذلك الدول التي عبر خلالها النشاط المجرم، أو في أي مكان قد توجد أدلة الجريمة فيه[1].

وتبعا لذلك و لأجل تفعيل المسار الإجرائي في مجال مكافحة الجريمة المعلوماتية فإن مظاهر التعاون الدولي و الإقليمي و الجهود الداخلية، ما فتئت تتظارف وتتكاثف في سبيل تحقيق نظام دولي

---

[1]– يوسف حسن يوسف – الجرائم الدولية للانترنت – الطبعة الأولى– المركز القومي للإصدارات القانونية – القاهرة– مصر– 2011 – ص 141.

إجرائي كفيل بسير إجراءات البحث و التحقيق في الجرائم المعلوماتية نظرا لطابعها الدولي ، وهو ما سنحاول تلخيصه لأجل الإجابة عن هذه الإشكالية في فرعين رئيسيين أولهما متعلق بالجهود الدولية في سبيل مكافحة الجريمة المعلوماتية و الثاني متعلق بالجهود على المستوى الإقليمي الأوروبي و العربي.

الفرع الأول:الجهود الدولية في سبيل دعم جهود مكافحة الجريمة المعلوماتية.

إن التطرق لجملة الجهود الدولية الموجهة لأجل دعم سبل مكافحة الجريمة المعلوماتية بما في ذلك أعمال البحث و التحقيق بشأنها، باعتبارها الإجراءات التي تتصادم مباشرة بالطابع الدولي لجرائم المعلوماتية مما يسفر عن تعطلها بسبب مبدأ إقليمية القوانين الجنائية ومفهوم سيادة الدول على إقليمها، ويمكن تلخيص هذه الجهود في جملة من الجهود التي ترعاها الأمم المتحدة و أخرى دولية.

الفقرة الأولى : جهود هيئة الأمم المتحدة في دعم مكافحة الجريمة المعلوماتية.

تبذل الأمم المتحدة جهودا لا يستهان بها في مجال التصدي لجرائم المعلوماتية ، وتؤكد على وجوب تعزيز العمل المشترك بين أعضاء المنظمة من أجل التعاون على الحد من انتشارها وتعاظم أثارها، فمن خلال تتبع المؤتمرات الدولية التي تنعقد بإشراف الأمم المتحدة و الخاصة بمنع الجريمة، فلقد حظيت جرائم الحاسب أو الجرائم المعلوماتية باهتمام وفير من خلال هذه المؤتمرات وهو ما سنحاول تبيانه من العرض التدريجي لجهود الأمم المتحدة في هذا المجال[1].

بعدما تم أنشاء منظمة الأمم المتحدة سنة 1945 اتخذ المجلس الاقتصادي و الاجتماعي التابع لها توصية بأن تأخذ المنظمة على عاتقها دورا رئيسيا في رسم سياسة منع الجريمة وتحقيق العدالة الجنائية دوليا، وتحقق ذلك بموجب توصية عام 1950 التي انبثق عنها اللجنة الاستشارية لخبراء منع الجريمة ومعاملة المجرمين التي تتكفل بمهمة مكافحة الجريمة و وضع الخطط و البرامج ورسم سياسات لتدابير

[1]- محمود أحمد عبابنة- جرائم الحاسوب وأبعادها الدولية- دار الثقافة للنشر و التوزيع- الأردن- 2005- ص 155.

دولية في مجال منع الجريمة و معاملة المجرمين ، و قد تم إستبدال اللجنة الإستشارية بلجنة منع الجريمة و مكافحتها بناء على توصية المجلس الاقتصادي و الاجتماعي عام 1981 وذلك بعد انعقاد مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة المجرمين في كيوتو اليابان عام 1980، هذه المؤتمرات التي تنعقد كل 05 سنوات تهدف إلى تعزيز تبادل المعرفة و الخبرات بين الأخصائيين من مختلف الدول و إلى تدعيم التعاون الدولي و الإقليمي في مجال مكافحة الجريمة، وقد كان المؤتمر السابع من هذا النوع المنعقد في ميلانو بإيطاليا عام 1985 أولى المؤتمرات التي صاغت أولى الجهود الدولية في مجال مكافحة الجريمة المعلوماتية من خلال دعم جهود حماية المعطيات و البيانات الشخصية المعالجة آليا.[1]

ويمكن تصنيف توصيات مؤتمر "هافانا" لعام 1990 طبقا لما أوردها الدكتور (عبود الشرع) كأهم التوصيات المقدمة من قبل هيئة الأمم المتحدة في مجال مكافحة الجرائم المعلوماتية و دعم الإجراءات الخاصة بالبحث و التحقيق بشأنها و قد جاءت كالتالي :

- ضرورة تحيين القوانين الجنائية الوطنية.
- العمل على تحسين أمن الأنظمة المعلوماتية
- اعتماد إجراءات تدريب كافة الموظفين و الوكالات المسئولة عن منع الجرائم المتعلقة بالحاسوب وجهاز البحث و التحري بشأنها.
- اعتماد سياسات تعالج المشكلات المتعلقة بالمجني عليهم في تلك الجرائم.
- زيادة التعاون الدولي لأجل مكافحة هذه الجرائم وهي التوصيات التي تأكدت من خلال المؤتمرات اللاحقة سنة 1995 بالقاهرة- مصر- وسنة 2000 بالمجر (بودابست) ومؤتمر 2005 ببانكوك.[2]

---

[1]- محمود أحمد عبابنة- مرجع سابق – ص 156،157.

[2]- المرجع السابق – ص 158،159.

كما اعتمدت الأمم المتحدة على ما يعرف بالخطوط التوجيهية لحماية المعطيات الشخصية المعالجة آليا، وذلك بموجب قرارها رقم 95/45 المؤرخ في 1990/12/14 وهي توجيهات متعلقة بالمعطيات الشخصية المعالجة آليا على مستوى القطاع العام و الخاص و كذلك الدولي، تدعو هذه التوجيهات كل الدول الأعضاء إلى تعيين سلطة للمراقبة مستقلة ومحايدة تشرف على تداول المعطيات مع توفير الضمانات الضرورية لحماية هذه المعطيات من كل أشكال التهديد[1].

وقد ناقش الدول الأعضاء بموجب اجتماعهم في البرازيل في أفريل 2010 مسألة كيفية مكافحة الجريمة المعلوماتية وذلك بالتأكيد على ضرورة إنشاء هيئة دولية لأجل مكافحة الجريمة المعلوماتية ترعاها الأمم المتحدة وذلك تجنبا لمسائل تنازع الاختصاص الإقليمي للقوانين الإجرائية الجزائية[2].

الفقرة الثانية :صور وآليات التعاون الدولي في مجال دعم مكافحة الجريمة المعلوماتية.

يمكن إيجاز مبادئ التعاون الدولي في مجال دعم أعمال البحث و التحقيق في الجرائم المعلوماتية في الصور التالية:

أولا: تبادل المعلومات: وهو إجراء يشمل تقديم المعلومات و البيانات و المواد الاستدلالية التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة ما، عن الاتهامات التي وجهت إلى رعاياها في الخارج و الإجراءات التي اتخذت ضدهم، وقد يشمل التبادل السوابق القضائية للجناة ولهذا الإجراء سند قانوني فهو منصوص عليه بالبند "و" و "ز" من الفقرة الثانية من المادة 01 من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية.

ثانيا: نقل الإجراءات: ويقصد به قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جزائية بصدد جريمة ارتكبت في إقليم دولة أخرى لمصلحتها، إذا توافرت شروط معينة أهمها التجريم المزدوج بالإضافة

[1]- فتوح الشاذلي – عفيفي كمال عفيفي- مرجع سابق – ص 27،28.

[2] -Myriam Quéméner- Yves Charpenel – La Cybercriminalité – op.cit.p 232.

إلى شرعية الإجراءات المطلوب اتخاذها، بمعنى أن تكون مقررة في قانون الدولة المطلوب منها اتخاذها إضافة إلى كونها إجراءات جوهرية في كشف الحقيقة ،وهو الإجراء المنصوص عليه في معاهدة الأمم المتحدة لنقل الإجراءات في المسائل الجنائية ،واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة 2000.[1]

ثالثا: الإنابة القضائية الدولية: يقصد بها طلب اتخاذ إجراء قضائي من أجل إجراءات الدعوى الجنائية تتقدم به دولة طالبة إلى دولة مطلوب منها، لضرورة الفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة تعذر عليها القيام به بنفسها، ويهدف هذا الإجراء إلى تسهيل المتابعة القضائية و التغلب على عقبات مبدأ الإقليمية[2].

الفرع الثاني: الجهود المحققة على المستوى الإقليمي.

نحاول في هذا الفرع التطرق إلى الجهود التشريعية وذلك على المستوى الإقليمي، و التي تهدف إلى دعم جهود مكافحة الجرائم المعلوماتية من خلال تيسير أعمال البحث و التحقيق بشأنها ويمكن اعتبار الجهود المبذولة على النطاق الأوروبي نموذجا يقتدى به في هذا المجال من قبل بقية الدول الأخرى وهو ما يجعل منه موضوعا مناسبا لبدء البحث.

الفقرة الأولى: الجهود المبذولة في سبيل التصدي للجرائم المعلوماتية على المستوى الأروبي.

في مجال الجهود الرامية للتصدي للجرائم المعلوماتية على المستوى الأوربي يمكن التمييز بين تلك الجهود الصادرة عن المجلس الأوربي وتلك الصادرة عن الإتحاد الأوربي.

---

[1]- يوسف حسن يوسف- مرجع سابق- ص 151،150.

[2]- المرجع السابق- ص 152.

أولا: دور المجلس الأوربي: يلعب المجلس الأوربي دورا مهما في الحد من الجرائم المعلوماتية من خلال إقراره للعديد من التوصيات الخاصة بحماية البيانات ذات الطبيعة الشخصية من سوء الاستخدام وحماية تدفق المعلومات، ففي 1981/01/28 وقعت الاتفاقية الخاصة بحماية الأشخاص في مواجهة المعالجة الإلكترونية للبيانات ذات الطبيعة الشخصية تحت رقم 108، تم التصديق عليها من قبل 17 دولة[1].

غير أن الحدث الأبرز في هذا المجال هو تتويج المجلس الأوروبي لجهوده من خلال إقراره لاتفاقية بودابست لمكافحة الجرائم المعلوماتية بتاريخ 2001/11/21 تحت رقم 185- و التي تهدف إلى عصرنة التشريعات الداخلية مع واقع عالم الرقمية، وقد عالجت هذه الاتفاقية كل المسائل المتعلقة بالجريمة المعلوماتية، وقد دخلت حيز التنفيذ بتاريخ 2004/07/01 وهي الاتفاقية التي تساهم بشكل دائم ومستمر في دعم جهود مكافحة الجرائم المعلوماتية[2].

وضعت هذه الاتفاقية للتوقيع و التصديق عليها حتى من قبل الدول خارج الإتحاد الأوربي، فهي اتفاقية ذات طابع دولي أكثر منه إقليمي وقد كانت محل تصديق من قبل 47 دولة ، وتوقيع من دون تصديق من قبل 07 دول وذلك حسب آخر تحديث مؤرخ في 19 ديسمبر 2015، وتعتبر "سيريلانكا" آخر دولة تصادق على هذه الاتفاقية بتاريخ 29 ماي 2015.

تهدف هذه الاتفاقية إلى ترسيخ مبادئ جنائية حديثة تتماشى و التطور المستمر و التغيرات العميقة التي حدثت بسبب انتشار التكنولوجيا الرقمية، وتضم هذه الاتفاقية في فصولها (48) نصا موزعا على ثلاث (03) محاور أساسية هي:

---

[1]- محمود أحمد عبابنة- مرجع سابق – ص 164.

[2] – Myriam Quéméner- Yves Charpenel – La Cybercriminalité – op.cit –p 228.

- **الأول:** يضم الجوانب الموضوعية لجرائم المعلوماتية من تحديد للمصطلحات الخاصة، وتحديد أركان ومفاهيم مختلف صور الجرائم المعلوماتية.
- **الثاني:** يضم الجوانب الإجرائية المتعلقة بآليات البحث و التحقيق في مجال الجرائم المعلوماتية.
- **الثالث:** يضم الأحكام المتعلقة بجرائم المعلوماتية العابرة للحدود، وقد دعمت هذه الاتفاقية بمذكرة تفسيرية صدرت قبل ذلك بتاريخ 2001/11/08 من قبل لجنة وزراء المجلس الأوربي بمناسبة الدورة رقم 109، إضافة إلى البروتوكول الإضافي للاتفاقية بودابست المتعلق بتجريم السلوكات الماسة بالكرامة الإنسانية، و المحرضة على أعمال العنف و الكراهية و العنصرية بواسطة الأنظمة المعلوماتية تحت رقم 189 بتاريخ 2003/01/28 بعد اجتماع المجلس الأوربي بستراسبورغ الفرنسية، وهو البروتوكول الذي كان محل تصديق من قبل 20 دولة وتوقيع من قبل 18 دولة أخرى وقد دخل حيز التنفيذ في 2006/03/01[1].

إضافة لكل ذلك فقد عمل المجلس الأوربي إلى وضع خطوط توجيهية شهر أفريل 2008، تهدف إلى دعم وتعزيز عمل الجهات المختصة بمكافحة الجرائم المعلوماتية كأجهزة الشرطة المختصة، و الأجهزة القضائية، وهو ما أكدته التوصيات المقدمة من قبل ورشة العمل للمجلس الأوربي المنعقدة سنة 2010 بقولها: " يجب العمل على:

- دعم الطابع الدولي لاتفاقية بودابست.
- تكوين رجل قضاء مختصين في مجال مكافحة الجرائم المعلوماتية.
- إعداد مخطط وخارطة لعمل أجهزة مكافحة الجرائم المعلوماتية.

---

[1]– La situation de la Convention sur la Cybercriminalité–Traité de Budapest – Disponible sur le site officiel du Conseil de l'Europe – Date de consultation : 03/06/2014– lien direct : http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=20/07/2014&CL=FRE

- تكثيف الجهود لردع الجرائم المتعلقة بالاستغلال الجنسي للأطفال عبر شبكة الانترنت[1].

ثانيا: دور الاتحاد الأوربي: يلعب الاتحاد الأوربي دورا فعالا في مجال دعم الجهود التشريعية على مستوى الإقليم الأوربي في مجال مكافحة الجرائم المعلوماتية وذلك من خلال الجهود التي يبذلها في هذا المجال اللجنة الخاصة و التي يمكن إيجازها في:

- القرار رقم JAI/68/2004 المتعلق بمكافحة الاستغلال الجنسي للأطفال عبر شبكة الانترنت.
- القرار رقم 222/2005/ JAI المتعلق بتحديد مجموعة السبل الفعالة في سبيل مكافحة الهجمات الإلكترونية ضد الأنظمة المعلوماتية.
- التقرير الصادر بتاريخ 2007/05/22 تحت عنوان " سياسة عامة في مجال مكافحة الجرائم المعلوماتية " و الذي تضمن مجموعة من الإجراءات الخاصة و الموجهة لتطوير ودعم سبل التعاون بين الجهات المختصة في مجال مكافحة الجرائم المعلوماتية وذلك على المستوى الأوربي وكذلك الدولي[2].

الفقرة الثانية: جهود الدول العربية في مواجهة الجرائم المعلوماتية.

تعتبر الجهود العربية في مجال دعم وترقية سبل التعاون فيما بينها من أجل التصدي ومكافحة الجرائم المعلوماتية، جهودا محتشمة مقارنة بجهود الدول الأوروبية، فقد كانت البدايات متمحورة حول دعم المواجهة الأمنية ضد الاعتداءات الماسة بحقوق المؤلف، على أساس عدم انتشار الجرائم المعلوماتية بعد في الأقطار العربية ويعد القرار رقم 229 لسنة 1996 الصادر عن اجتماع مجلس وزراء العدل العرب كأول قانون مقترح لمكافحة الجرائم المعلوماتية.

غير أن أهم الجهود العربية في هذا المجال هو مضمون الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المنبثقة عن اجتماع مجلس الوزراء الداخلية و العدل العرب بصفة مشتركة، بمقر الأمانة

---

[1]–Myriam Queménér– Yves Charpenel – La Cybercriminalité – op.cit –p 229.

[2]– Ibid– p 230.

العامة لجامعة الدول العربية بالقاهرة بتاريخ 2010/12/21. و التي كانت محل توقيع 23 دولة عربية بنفس التاريخ بما فيها الجزائر و التي تضمنت 05 فصول رئيسية هي:

- الفصل الأول: تضمن الأحكام العامة (المصطلحات).
- الفصل الثاني: تضمن الأحكام المتعلقة بالتجريم.
- الفصل الثالث: تضمن الأحكام الإجرائية الخاصة بالبحث و التفتيش.
- الفصل الرابع: تضمن الأحكام الخاصة بالتعاون القضائي ومبادئ الاختصاص.
- الفصل الخامس: تضمن الأحكام الختامية.

وتعتبر هذه الاتفاقية نموذجا يحاكي الاتفاقية الأوروبية لمكافحة الجرائم المعلوماتية من خلال التفصيل الوارد في مضمونها لكل المسائل الخاصة بإجراءات البحث و التحقيق المعلوماتي.[1]

غير أن ما يعاب على جملة الدول العربية الموقعة على هذه الاتفاقية هو عدم التصديق عليها بعد من قبل العديد من الدول، عدا البعض منها كالمملكة البحرينية و السعودية اللتان توجتا ذلك بإقرار قوانين داخلية خاصة لمكافحة الجرائم المعلوماتية بصفة راعى فيها كل من المشرع السعودي و البحريني أحكام الاتفاقية العربية بشكل مطابق، وهو ما حاول المشرع الجزائري تنفيذه غير انه إستبق إقرار القانون 09-04 المتعلق بمكافحة الجرائم المعلوماتية بتاريخ 05 اوت 2009 قبل التصديق على مضمون الإتفاقية الذي تم بتاريخ 08 سبتمبر 2014 بموجب صدور المرسوم الرئاسي 14-252 و المنشور بالجريدة الرسمية العدد 57 لسنة 2014 و هو ما يفسر جوانب القصور التي تشوب القانون 09-04 حسب ما سنستعرضه في الفرع الموالي.

---

[1]- وثيقة الإتفاقية العربية لمكافحة جرائم تقنية المعلومات – لمزيد من التفاصيل راجع الملحق رقم :**04**

الفرع الثالث: جهود المشرع الجزائري في مجال دعم مكافحة الجرائم المعلوماتية.

في إطار الجهود الدولية و الإقليمية المتعلقة بترقية ودعم سياسة مكافحة الجرائم المعلوماتية، بما فيها دعم وتسيير أعمال البحث و التحقيق، عمل المشرع الجزائري على مسايرة النسق التشريعي، لأجل البقاء على اتصال بأحدث الحلول التشريعية الخاصة بهذا النوع من الجرائم خصوصا و أن الجزائر تعرف مؤخرا وفي السنوات الأخيرة تعميم خدمة الربط بشبكة الانترنت، ودعم الجهات الحكومية بتقنيات المعلوماتية، وهو ما تولد عنه ارتفاع محسوس في معدلات الجريمة المعلوماتية، وهي المعطيات التي دفعت بالمشرع الجزائري إلى التدخل من أجل رسم الخطط القانونية و العملية لتنفيذ سياسة وقائية وردعية ضد الجرائم المعلوماتية، وقد كان أول تشريع خاص بهذا المجال قد صدر بتاريخ 2004/11/10 بموجب القانون 04-05 المعدل و المتمم لقانون العقوبات الجزائري من خلال إقرار واستحداث قسم خاص معنون بقسم جرائم المساس بأنظمة المعالجة الآلية للمعطيات و الذي حمل بين طياته نصوص المواد من 394 مكرر إلى 394 مكرر 07، والتي تضمنت في فحواها صور الجرائم المعلوماتية من جرائم دخول غير مشروع إلى جرائم مساس بأمن وسلامة النظم المعلوماتية العامة و الخاصة منها إضافة إلى تحديد مقدار العقوبات المناسبة لها.

غير أن هذا الجهد لم يكن كافيا لتفعيل سياسة مكافحة الجرائم المعلوماتية بسبب تعارض أحكام قانون العقوبات وقانون الإجراءات الجزائية وخصوصا مسائل الاختصاص النوعي و الإقليمي التي وقفت عائقا في وجه تطبيق النصوص العقابية، مما استدعى تدخل المشرع الجزائري بموجب القانون 06-22 المؤرخ في 2006/12/20 المعدل و المتمم لأحكام قانون الإجراءات الجزائية الجزائري و الذي تناول بالتعديل و التحديث نصوص المواد من 45 إلى 47 منه و التي تحدد قواعد الاختصاص النوعي

و المحلي ومواعيد إجراء التفتيش بشأن الجرائم المعلوماتية، وهي الإجراءات التي سوف نتناولها بالتفصيل في المطلب الأول من المبحث الأول من الفصل الثالث لبحثنا هذا.

ولعل أن ما يجب الإشارة إليه في هذا الصدد هو القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام[1] و الاتصال ومكافحتها الصادر بتاريخ 2009/08/05 تحت رقم 09-04 و الذي يعتبر نموذجا قانونيا خاصا بمكافحة الجرائم المعلوماتية على اعتبار أنه قانون يتضمن نصوصا خاصة في هذا الشأن ، وقد تضمن هذا القانون 19 نصا موزعا على ستة (6) فصول.

- الفصل الأول تضمن الأحكام العامة الخاصة بالعمل بهذا القانون، كأهدافه و المتمثلة أساسا في وضع قواعد خاصة بالوقاية من الجرائم المعلوماتية إضافة إلى تحديد قائمة المصطلحات المفتاحية، وتحديد مجال تطبيق أحكامه.
- الفصل الثاني تضمن بيان مفهوم المراقبة الإلكترونية
- الفصل الثالث فقد حدد القواعد الإجرائية لعمليات التفتيش الإلكترونية وكيفيات حجز الأدلة الإلكترونية.
- الفصل الرابع فقد حدد جملة الالتزامات الملقاة على عاتق مقدمي خدمات الانترنت في مجال مساعدة السلطات بشأن التحقيقات الجنائية في مادة الجرائم المعلوماتية.
- الفصل الخامس: حدد مهام الهيئة الوطنية للوقاية من الجرائم المعلوماتية.
- الفصل السادس المحدد لقواعد الاختصاص القاضي في مجال التعاون الدولي في مسائل البحث و التحقيق في الجرائم المعلوماتية.

[1] – يجب الإشارة انه كان من الأجدر على المشرع الجزائري استعمال مصطلح "المعلوماتية" بدل "الإعلام" لأن جرائم الإعلام لها قانون خاص ينظمها و هو قانون الإعلام و لا علاقة لهذا المصطلح بالجرائم المعلوماتية و بالتالي وجب التدخل لأجل إعادة ضبط المصطلحات بدقة.

ويعتبر هذا القانون نموذجيا متكاملا من حيث نصوصه وجملة المبادئ التي وضحها في مجال مكافحة الجرائم المعلوماتية وتسيير أعمال البحث و التحقيق ، غير أن ما يعاب عليه هو الجمود الذي ميزه منذ سنة 2009، بحيث اكتفى المشرع بوضع النصوص دون أن يهتم بتطويرها و تحديثها منذ ذلك الحين، غير مدرك بأن قطار الجرائم المعلوماتية لا يتوقف وهو آخذ بالتقدم بوتيرة سريعة نظرا لتطور تكنولوجيا المعلوماتية المذهل و الذي يستغل جانب منه في مجال الإجرام المعلوماتي ، وبناء على ذلك وجب على المشرع الجزائري تحديث النصوص من أجل ضمان مكافحة فعالة للجرائم المعلوماتية .[1]

و تعتبر آخر الجهود في هذا المجال صدور المرسوم الرئاسي رقم 15-261 بتاريخ 08 أكتوبر 2015 المتضمن إنشاء الهيئة الوطنية المكلفة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها ، التي تتولى الإشراف على عمليات البحث و التحقيق في مجال الجرائم المعلوماتية، و دعمها تقنيا من خلال النص على إنشاء وحدة عملية تعرف بـ " مديرية المراقبة الوقائية و اليقظة الإلكترونية " تعمل بدعم من " مركز للعمليات التقنية " و ملحقات جهوية على تذليل العقبات التي تواجه المحققين في مجال الوقاية و مكافحة الجرائم المعلوماتية، وفق مجموعة من الأحكام القانونية تحددها ثلاث و أربعون (43) مادة قانونية تشكل الإطار القانوني لعمل الهيئة ، و يعتبر هذا المرسوم الرئاسي مكملا أساسيا لقانون 09-04 ، غير ان ما يعاب عليه هو طول مدة صدوره و التي كان من المفترض ان تلي صدور القانون 09-04 سنة 2009 ، و لكنها إمتدت إلى غاية شهر أكتوبر 2015 و هو ما خلق فراغا تشريعيا و تسبب في تعطيل أعمال البحث و التحقيق في مجال الجرائم المعلوماتية طيلة تلك المدة .

[1] – لمزيد من التفصيل راجع الملحق رقم : **02**

إذن فما يمكننا قوله ختاما ان الجريمة المعلوماتية قد أصبحت ضمن الإنشغالات الرئيسية لفقهاء القانون و المشرعين و المهتمين بالمجال الأمني ، و ذلك على كافة الأصعدة من أجل إيجاد الحلول اللازمة لمجابهتها ، و في مقدمتها إيجاد السبل و الآليات القانونية الشرعية التي تطور من نوع و فعالية الإجراءات الخاصة سواء بمرحلة البحث و التحري أو مرحلة التحقيق في مجال الجرائم المعلوماتية ، و هي بذلك فقد حازت على الإعتراف الفقهي و القانوني بشرعية الإجراءات المتخذة بشأنها إجرائيا ، و هو ما إنعكس في صورة ظهور و إستفراد وحدات و هيئات خاصة دون سواها بمهام البحث و التحقيق .

المبحث الثاني: الهيئات المختصة بمهام البحث و التحقيق في الجرام المعلوماتية.

يخضع أمر البحث و التحري و التحقيق المعلوماتي إلى جهات مختصة غير تلك التقليدية متمثلة في جهات أمنية مختصة و أخرى قضائية ، وقد تكون حتى جهات خاصة مستقلة، تضع خبرتها وكفائتها تحت تصرف الجهات الأمنية و القضائية في سبيل مساعدتها على كشف خيوط الجريمة المعلوماتية، وتحديد هوية مرتكبها بالرغم من تعقيدات الأمر من الناحية التقنية بالنظر إلى طبيعة الجريمة المعلوماتية، وطبيعة الأدلة الناتجة عنها، و التي من النادر أن يتغافل الجاني عن تركها وراءه، وبناء على ذلك فإن أمر البحث و التحقيق تتولاه جهات من نوع خاص من حيث التركيبة البشرية المكونة لها و التي يتمتع أفرادها بعاملي الخبرة العملية و الكفاءة في مجال النظم المعلوماتية، وإلمامهم بجرائم المعلوماتية، وهو ما يسمح لهم بالتحكم في مجريات التحقيق من خلال إجادتهم التعامل مع الوسائل الموضوعة تحت تصرفهم من أجهزة الحواسيب و البرامج و النظم الخاصة، و التي تسمح لهم بملاحقة المجرمين المعلوماتيين، واقتفاء أثرهم الإلكتروني، فمن الصعب و من المستحيل على رجال البحث و التحقيق في الجرائم التقليدية التعامل مع الجرائم المعلوماتية، وهو ما يقتضي ضرورة استحداث وحدات خاصة لأجل مجابهة فئة مجرمي المعلوماتية، على اعتبار أنهم الفئة الأخطر من الناحية الإجرامية على أمن وسلامة النظم المعلوماتية، نظرا لخصوصياتهم وقدراتهم الفائقة على إخفاء أثار جرائمهم .

إن أمر استحداث وحدات خاصة لمكافحة الجرائم المعلوماتية، ودعم وسائل البحث و التحقيق بشأنها، أضحى أمرا ضروريا لا مفر منه على عاتق الجهات الأمنية و القضائية، وذلك بالنظر إلى تفاقم الظاهرة الإجرامية المعلوماتية من يوم لآخر، وكذلك نظرا لزيادة مدى خطورتها و أساليبها إضافة إلى اتساع رقعة نشاطها لتشمل كل من هو موصول بالشبكة سواء هيئات عمومية أو خاصة أو أفراد.

ولقد كانت الدول الغربية السابقة في مجال استحداث وحدات مختصة بمكافحة المعلوماتية نظرا لباعها الطويل مع هذه التقنية ومعاناتها بشكل كبير من آثارها السلبية، وذلك عكس الدول العربية و النامية التي لا زالت تعاني قصورا تشريعيا حول تجريم الأفعال الماسة بأمن النظم المعلوماتية، وهو ما يشكل عائقا في وجه توحيد الجهود على كل المستويات من أجل ضمان مكافحة فعالة للجرائم المعلوماتية.

وسنحاول استعراض في مبحثنا هذا بالدراسة على امتداد ثلاث 03 مطالب أهم الهيئات المختصة بمكافحة الجرائم المعلوماتية ، وذلك على المستوى الدولي (المطلب الأول) و المستوى الأوروبي متخذين النموذج الفرنسي كنموذج مقارن للدراسة (المطلب الثاني)، و على مستوى الدول العربية و التشريع الجزائري خصوصا في (المطلب الثالث).

المطلب الأول: الهيئات الدولية المختصة بمسائل البحث و التحقيق في الجرائم المعلوماتية.

إن الطابع الدولي للجريمة المعلوماتية وعدم اعترافها بمفهوم الحدود الإقليمية، بفعل اتساع شبكة الانترنت التي أضحت تغطي كل بقاع الأرض، وعدم وجود ضوابط مادية تسمح بتحديد نطاق الإبحار عبر هذه الشبكة، جعل من أمر التهديد المعلوماتي الدولي أمرا واقعا، فيمكن للمجرم المعلوماتي أن ينفذ جريمة وهو في غير موطن الضحية بل يبعد عنه بآلاف الكيلومترات، وهو ما يفسر التنامي اللامحدود للاعتداءات المعلوماتية، التي تستهدف النظم المعلوماتية لكبرى المؤسسات و الهيئات الحكومية، من قبل قراصنة

الانترنت على المستوى الدولي ونذكر في هذا الشأن مثالا، فالنظام المعلوماتي لهيئة الدفاع الأمريكية يشكل أكثر النظم تعرضا للهجوم الإلكتروني من كل بقاع الأرض بهدف اختراقه، وذلك من قبل مجموعات من الهاكرز إما بهدف التباهي أو إثبات الذات، أو تلك الهجمات الداخلة في إطار الحرب الإلكترونية القائمة بين معسكري الشرق و الغرب[1].

أما على المستوى الأوروبي فيمكن أن نستشهد بما تعرض له النظام المعلوماتي الخاص باللجنة الأوروبية في 23 مارس 2011، ليلة اجتماع رؤوساء الوزراء الأوربيين من خلال تعرضه لهجوم إلكتروني بواسطة فيروس غير معروف بهدف شله عن العمل[2].

إن كل هذه التهديدات و الاعتداءات الإلكترونية، دفعت بهذه الدول إلى استحداث هيئات ووحدات وأقسام خاصة بمكافحة الجرائم المعلوماتية، و العمل على تطويرها بشكل يسمح لها بالتحكم في هذه الظاهرة، على كافة الأصعدة بما فيها الإجرائية خصوصا وذلك على المستوى الدولي، وتعتبر الهيئات الأوروبية رائدة في هذا المجال بالنظر إلى قدرتها على التعامل مع هذه المسائل من خلال استحداث الهيئات التالية:

- هيئة الأنتربول (الفرع الأول).
- هيئة الأوروبول (الفرع الثاني).
- هيئة الأوروجيست (الفرع الثالث).

---

[1] –Feverier Rémy–Management de la sécurité des systèmes d'information : les collectivités territoriales face au risque numérique– Thèse de Doctorat– Ecole Doctoral de science Economique et de gestion– université Paris 02– France – Avril 2012–p 89.

[2] – Ibid – p 92.

فما هي يا ترى طبيعة هذه الهيئات؟ وما هي مجالات اختصاصها في ميدان البحث و التحقيق المعلوماتي على النطاق الدولي؟

الفرع الأول:هيئة الأنتربول.

تعتبر هيئة الأنتربول بمثابة الشرطة المختصة بمكافحة الجريمة و ملاحقة المجرمين على المستوى الدولي ، عملا منها على تحقيق العدالة و الأمن الدوليين ، في ظل تصاعد التهديدات الإجرامية ، و أثرها على إستقرار و أمن المجتمعات ، و لم تصل هذه الهيئة إلى هذه الدرجة من الوعي الأمني إلا من خلال تبني مجموعة من المبادئ و العمل على تدعيمها بوسائل مادية تساعدها في تحقيق هذه الأهداف ، و ذلك على مد من الزمن نحاول إيجازه فيما يلي من فقرات :

الفقرة الأولى: نشأة الأنتربول و أهدافه العامة.

أبصرت فكرة الأنتربول النور عام 1914 خلال المؤتمر الدولي الأول للشرطة الجنائية الذي عقد "بموناكو" ‘MONACO’ الفرنسية، وقد شارك في هذا المؤتمر موظفو وممثلو الأجهزة القضائية من 24 دولة لإيجاد سبل التعاون لحل الجرائم و لاسيما ما تعلق بإجراءات البحث و التحقيق وتوقيف المجرمين وتسليمهم، وقد أنشأت المنظمة الدولية للشرطة الجنائية (الأنتربول) رسميا عام 1923، وازداد عدد الدول المنتمية لها على مر السنوات ليصل إلى 190بلدا أجنبيا، ولا تزال رؤية الأنتربول تتماشى و الأهداف الأساسية التي وضعت عام 1914، وذلك في مواجهة الاتجاهات الحديثة للجريمة وانتشار الطابع الدولي للجرائم ، و تتمثل مهمة الأنتربول في تمكين أجهزة الشرطة حول العالم أجمع من العمل معا لمنع الجريمة الدولية ومكافحتها من خلال تحقيق الأهداف التالية:

- الوصل بين أجهزة الشرطة حول العالم لجعلها أكثر أمنا، لأجل منع الجريمة ومكافحتها عبر تعزيز التعاون الشرطي الدولي.

- توفير الدعم على مدار الساعة لأجهزة الشرطة وإنفاذ القانون.
- بناء القدرات من خلال توفير دورات تدريبية للارتقاء بمعايير عمل أجهزة الشرطة.
- كشف الجرائم و المجرمين من خلال توفير قاعدة بيانات دولية، وقدرات تحليلية وأدوات مبتكرة على أعلى مستوى من الجودة للمساعدة على منع الجريمة.
- مساعدة البلدان الأعضاء على تبين الأشخاص الفارين و المجرمين وتحديد مكان وجودهم وتوقيفهم.
- ضمان استمرارية الأعمال من خلال تعزيز البنى التحتية الأساسية للأنتربول وتحسين نمط عمل المنظمة[1].

الفقرة الثانية: جهود الأنتربول في مجال تطوير وسائل البحث و التحقيق في الجرائم المعلوماتية.

تباشر منظمة الأنتربول وظيفتين رئيسيتين في جال مكافحة الجرائم الأولى تتمثل في تجميع كافة البيانات و المعلومات المتعلقة بالجريمة و المجرم من خلال عمل المكاتب المركزية الوطنية للشرطة الجنائية الدولية المتواجدة على إقليم الدول الأعضاء، أما الثانية فتتمثل في التعاون في ملاحقة المجرمين وتسليمهم إلى الدول التي تطلبهم، وهي بذلك متخصصة بمكافحة الجرائم ذات الطابع الدولي وخصوصا جرائم الاستغلال الجنسي للأطفال عبر شبكة الانترنت، وفي هذا السياق نجد دعوة سكرتيرتها RAYMOND–KENDALL في مؤتمر جرائم الانترنت المنعقد في لندن في 2000/10/09 بضرورة إيجاد تعاون دولي لمكافحة هذا النوع من الإجرام، وهو ما أكده مديرها التنفيذي للخدمات الشرطية السيد (LEBOTANE) في المؤتمر الدولي السادس بشأن الجرائم المعلوماتية المنعقد بالقاهرة–أفريل 2005،

---

[1]– "لمحة عن الأنتربول"– بحث متوفر على الموقع الرسمي للأنتربول الدولي– النسخة العربية–تاريخ التصفح : 25–05 –2014 – الرابط الإلكتروني :

http://www.interpol.int/content/download/785/342162/version/22/file/01_GI01_03_2014_AR_web.pdf

وكذلك الحال بالنسبة لما جاء على لسان المدير العام لمركز بحوث الشرطة الأسترالية (DESBERWICK) الذي دعى إلى ضرورة القيام بالتحقيق في الجرائم المعلوماتية بطريقة متزامنة في العالم أجمع[1].

وفي سبيل تجسيد ذلك نظمت الأنتربول شهر فيفري من سنة 2005 المؤتمر الثاني للتنسيق بشأن جرائم الاحتيال المعلوماتي، و التي دعى إليها بعد وقوع 2000 شخص ضحية من مجموع 60 دولة مختلفة قدرت خسائرهم بحوالي 166 مليون أورو، وقد ألقي القبض على المتهمين بشأنها في ديسمبر 2004 في اسبانيا بعد تقدم النائب العام الألماني بطلب المساعدة الدولية من قبل الأنتربول، وفي سبيل مواصلة الجهود بشأن ذلك وتأكيدا لما دعى إليه مؤتمر القاهرة نظم الأنتربول شهر سبتمبر 2005 بمدينة ليون الفرنسية المؤتمر الدولي الأول لتكوين المحققين في الجرائم المعلوماتية و الذي عرف مشاركة و إرسال 30 دولة لخبرائها من أجل الاستفادة من هذا التكوين[2].

الفقرة الثالثة: وسائل الأنتربول المادية للمساعدة في أعمال البحث و التحقيق المعلوماتي.

لا يقتصر عمل الأنتربول في مجال مكافحة الجريمة المعلوماتية، في صور عقد واحتضان المؤتمرات الدولية بل يعمل الأنتربول لأجل تجسيد ذلك ميدانيا ، من خلال العمل على دعم إجراءات البحث و التحقيق بشأنها من خلال :

- جمع وتخزين وتحليل المعلومات المتعلقة بالجرائم المعلوماتية مع توفيرها لكافة الدول الأعضاء بواسطة منظومة I24/7 للأنتربول، وهي عبارة عن شبكة اتصالات شرطية مأمونة تربط بين الدول الأعضاء[3].

---

[1]- نبيلة هبة هروال- مرجع سابق- ص 151- 152.

[2]-Mohamed Chawki – Combattre la cybercriminalité – Edition de saint Amans- Paris – France- Mai 2009- p 343.

[3]- Myriam Quéméner- Yves Charpenel – La Cybercriminalité – op.cit- p 208.

- هذه الشبكة التي تم تطويرها من خلال دعمها بمنظومة I-Link التي تعتبر المركز الرئيسي لتبادل المعلومات الجنائية و التواصل بين الدول الأعضاء، وهي منظومة اتصالات محسنة مقارنة بمنظومة I24/7، وتتضمن عددا من الوظائف التي تضمن نقل وتبادل المعلومات الشرطية تبادلا فعالا من خلال:
- استحداث معيار منسق للاتصالات لتسهيل تبادل المعلومات الشرطية.
- إمكانية التحكم المباشر في البيانات و التدقيق فيها.
- إمكانية تسجيل أحدث المعلومات مباشرة في قاعدة البيانات الجنائية.
- توفير أداة بحث قوية وسريعة فعالة تضمن حصول الشرطة على الإجابات الفورية و الشاملة حول تقصيتها ، ويتمثل الهدف النهائي لهذه المنظومة في نقل جميع المعلومات الجنائية المتبادلة عن طريق الأنتربول في شكل رسائل منسقة تجعل من أمر التقصي على قدر كبير من السهولة[1].

إضافة لذلك يسهر الأنتربول على:

- تسيير قاعدة البيانات الجنائية الدولية I-Link و I24/7 .
- تقديم الدعم لمصالح الشرطة على المستويين الدولي و الداخلي.
- تكوين وتطوير أعوان الشرطة بحيث تنظم دورات تكوينية تسمح لأعوان الشرطة تحسين قدراتهم على التعامل مع منظومة الاتصال I24/7 و I-Link في إطار سياسة التعاون الدولي لمكافحة الجرائم المعلوماتية[2].

---

[1]- "منظومة I-Link الربط بين التحقيقات في العالم أجمع"- بحث متوفر على الموقع الرسمي للأنتربول -النسخة العربية- ص 10،11- تاريخ التصفح: 2014/08/08- الرابط الإلكتروني :
http://www.interpol.int/content/download/789/342185/version/21/file/05_GI05_08_2013_AR_web.pdf.

[2]-Céline Renard Castétes – Cours de Droit de l'internet – Edition 2010 – Edition – Lex tenso – Paris – France- 2010 P : 563-564.

إضافة لذلك فإن منظمة الأنتربول تعمل دوما و بالتنسيق مع الدول الأعضاء من أجل القيام بعمليات نوعية تستهدف الإجرام المعلوماتي، كعملية أنماسك (ANMASK) و التي استهدفت قراصنة الحواسيب على المستوى الدولي و التي أسفرت عن اعتقال 25 شخصا في أمريكا اللاتينية و أوروبا، وذلك بتضافر جهود كل من إسبانيا، الأرجنتين، تشيلي، كولومبيا، وذلك عقب سلسلة الاعتداءات المعلوماتية المنسقة و التي انطلقت من هذه الدول ضد مواقع إلكترونية حكومية كولومبية[1].

الفرع الثاني: هيئة الأوروبول L'EUROPOL

يعتبر الأوروبول وليد ونتاج سيطرة الأنتربول على الساحة الأوروبية لمدة طويلة من الزمن، وقد قدم الطرح المتعلق بإنشاءه أول مرة أمام المجلس الأوربي من قبل ألمانيا سنة 1991، بمناسبة انعقاد مؤتمر لوكسمبورج، غير أنه تجسد فعليا سنة 1995، وذلك بعد مصادقة دول المجلس الأوربي على اتفاقية ماستريخت في 1995/07/29 ليتخذ من لاهاي مقرا له[2].

يتكفل الأروبول بمكافحة الإجرام عن طريق معالجة المعلومات المرتبطة بالأنشطة الإجرامية على مستوى الإتحاد الأوربي، ودعم وتشجيع سلطات التحقيق وذلك بتكميل وسائلهم وتجديدها من أجل مكافحة جميع أنواع الإجرام المنظم الدولي، وكذلك من خلال تسهيل تبادل المعلومات عن طريق تزويد المحققين بتحاليل علمية وإستراتيجية ودعمهم بالخبرات و المساعدة التقنية[3].

يعتبر الأوروبول من أكبر الهيئات الاستشارية حول العالم في مجال الجرائم المعلوماتية، من خلال دعمه للحكومات و الأجهزة الأمنية و المؤسسات في مسارها ضد أخطار الجرائم المعلوماتية، وقد تم اختياره من

---

[1]– التقرير السنوي لنشاط الأنتربول لسنة 2012– متوفر على الموقع الرسمي للأنتربول–النسخة العربية– تاريخ التصفح: 2014/04/12– الرابط الإلكتروني:
http://www.interpol.int/content/download/20552/185417/version/5/file/Annual%20Report%202012_AR_i.pdf

[2]– Céline Renard Castétes– op.cit –p 564.

[3]– نبيلة هبة هروال– مرجع سابق– ص 158.

قبل الاتحاد الدولي للأمن المعلوماتي، لإنجاز مختلف الدراسات الخاصة بالجريمة المعلوماتية وذلك إلى غاية سنة 2020، بهدف تحليل دوافع الجرائم المعلوماتية، ووضع تصور مستقبلي لتطورها، وهو ما يفسر الثقة التي وضعتها فيه اللجنة الأوروبية باختيارها له كمركز إعلام حول موضوع الجرائم المعلوماتية[1].

يختص الأوروبول وفي مجال مكافحة الجرائم المعلوماتية، بكل أشكال الإجرام التي ترتكب بواسطة التكنولوجيا الرقمية، تكون إحدى المنظمات الإجرامية الناشطة على الإقليم الأوروبي طرفا فيها[2].

ولذلك يرصد الأوروبول هيكلا بشريا يضم أكثر من 600 شخص بلاهاي يضمنون التنسيق و الدعم للمحققين الميدانيين سواء تعلق الأمر بدعمهم بالبيانات اللازمة أو التقنيات في مجال التحقيق[3].

وقد شهد الأوروبول سنة 2008 طفرة نوعية في وسائل عمله و صلاحياته فبتاريخ 24 أكتوبر 2008تقرر بلكسومبورغ إنشاء قاعدة بيانات أوروبية مشتركة بميزانية أولية قدرها 300.000€ تخضع لتسيير منظمة الأوروبول، وتضمن التنسيق بين عمل جهات الشرطة للدول الأعضاء من خلال إحصاء وجمع كافة القضايا الإجرامية التي لها علاقة بالمعلوماتية وذلك لأجل التنسيق بين عمل الجهات الأمنية[4].

وتطبيقا لذلك فقد اعتمد مجلس الوزراء الأوربي المنعقد ببروكسل بلجيكا في 2000/11/22، بمناسبة مناقشة مشروع télécom paquet فكرة منح الأوروبول صلاحية ومهمة ملاحقة ومتابعة مجرمي

---

[1] –Myriam Quéméner– Jean Paul Pinte – Cybersécurité– Edition Hermès science– Lavoisier– Paris– France 2013– p 194–195.

[2] –Myriam Quéméner – Joël Ferry– Cybercriminalité Défi mondial– Edition Economica – Paris – France–2009– p 237.

[3] – Myriam Quéméner– Yves Charpenel – La Cybercriminalité – op.cit– p 209.

[4] – Myriam Quéméner – Joël Ferry– Cybercriminalité Défi mondial– op.cit– p 238.

المعلومات، من خلال إعتماد أسلوب الدوريات الإلكترونية من ذلك بتجميع المعلومات التي يوفرها مزودو الخدمة بالانترنت وقوات الشرطة[1].

وفي الأخير يمكننا القول بأن الأوروبول مختصة بالبحث و التحقيق في الجرائم المعلوماتية خصوصا تلك المتعلقة بالاستغلال الجنسي للأطفال و الإرهاب الإلكتروني، وهو يهدف من خلال نشاطه إلى تسهيل الإجراءات أمام رجال الشرطة لأجل التحري بشأن الجرائم المتعلقة ببلدانهم، من خلال مدهم بمختلف النشرات الأمنية و التقارير حول هوية المتهمين و الأدلة المحصلة خارج الحدود الإقليمية لمجال اختصاصهم[2].

الفرع الثالث: هيئة الأوروجست L'EUROJEST

هو هيئة تعمل على مد يد العون و التنسيق بين الجهات القضائية الأوروبية، أنشأ سنة 2002 من قبل مجلس الإتحاد الأوروبي بتاريخ 2002/02/22، بهدف ضمان مناخ أمني و الحرية و العدالة، كما يعمل على تطوير آليات مكافحة الجريمة المعلوماتية من خلال تبادل المعلومات بصفة دورية مع محاكم الإتحاد الأوروبي[3].

و تجدر الإشارة إلى أن الأوروجست يمثل دعامة في فعالية التحقيقات و المطاردات، و المتابعة من قبل السلطات القضائية الوطنية وخصوصا فيما يتعلق بالأنشطة المرتبطة بالجرائم المعلوماتية، فهو يمهد للأوروبول عمله، في مجال التحقيق من خلال مده بالتحليلات اللازمة، ويتكون هيكله البشري من نواب عامين، ومستشارين قضائيين، وضباط الشرطة القضائية لمختلف الدول الأعضاء في الإتحاد الأوروبي الذين لهم صفة الاختصاص بحكم ندبهم من قبل كل دولة وفقا لنظامها القانوني[4].

---

[1] – Céline Renard Castétes– op.cit–p 564.

[2]– Myriam Quéméner – Joël Ferry– Cybercriminalité Défi mondial– op.cit– p 238.

[3] Myriam Quéméner– Jean Paul Pinte – Cyber sécurité– op.cit– p 195.

[4]– نبيلة هبة هروال – مرجع سابق– ص 160.

تختص الأوروجست بالمتابعة و التحقيق بشأن نفس الجرائم التي يختص بها الأوروبول، مع اختصاصه بمتابعة الجرائم المعلوماتية وجرائم الغش و الرشوة و تبييض الأموال، و الجرائم المتصلة بها، وذلك إذا ما تعلق الأمر بجرائم يكون طرفا فيها على الأقل دولتين من دول الاتحاد الأوروبي أو دولة واحدة إذا ما تعلقت مصالحها بمصالح الإتحاد الأوروبي وبذلك فهو زيادة على اختصاصه بمتابعة الأشخاص فإنه يشمل كذلك المؤسسات[1].

ويحكم عمل الأروجست في مجال متابعة الجرائم المعلوماتية ثلاث (03) أهداف رئيسية هي:

- تطوير وتحسين وسائل التنسيق في مجال المتابعة وذلك بين السلطات المختصة للدول الأعضاء.
- تسهيل التعاون بين الجهات القضائية في مجال المتابعات من خلال تنفيذ أوامر المساعدة القضائية الدولية، و الاستجابة لطلبات الإبعاد.
- دعم السلطات الوطنية من أجل ضمان فعالية المتابعة الجزائية[2].

إذن هذه هي الهيئات المختصة بإجراءات البحث و التحقيق في الجرائم المعلوماتية على المستوى الدولي و الظاهر بأنها كلها نتاج جهود أوروبية بالدرجة الأولى، وهي الهيئات التي نتمنى أن تكون متوفرة على مستوى الدول العربية و الإفريقية لأجل دعم الجهود المتعلقة بمكافحة الإجرام المعلوماتي على مستوى إقليمي خصوصا وأن الهيئات السالف ذكرها تركز جهودها في النطاق الأوروبي و الأمريكي و الشرق الآسيوي ، وسنستعرض تباعا وفي المطلب الموالي الجهات المختصة بمكافحة الجرائم المعلوماتية على المستوى الداخلي لعديد الدول واخترنا في ذلك المثال الفرنسي من بينها كعينة بحث خاصة .

---

[1]– Céline Renard Castetes – op.cit–p 570.

[2]– Myriam Quéméner – Joël Ferry– Cybercriminalité Défi mondial – op.cit– p 239.

المطلب الثاني: الجهات المكلفة بالبحث و التحقيق في الجرائم المعلوماتية على مستوى التشريعات المقارنة.

أمام تزايد الخطر في معدلات الجريمة المعلوماتية، وتسارع وتيرتها وامتداد أثارها إلى مستويات أعلى، فانتقلت التهديدات من مجرد قرصنة وتعطيل حواسيب الغير، إلى قرصنة وتعطيل الأنظمة المعلوماتية للحكومات برمتها، وأكبر المؤسسات المالية و التجارية على الصعيد الدولي، بما تحتويه هذه الأخيرة من معلومات وبيانات سرية، متعلقة بطبيعة نشاطها ومعاملاتها أو تلك الخاصة بزبائنها، وهي التهديدات التي تنجر عنها خسائر مالية كبرى نظرا لحساسية هذه المعطيات، وكما سبق وأن رأينا أنه هناك هيئات دولية تعمل في مجال مكافحة الجريمة المعلوماتية، من خلال دعم جهود تيسير إجراءات البحث و التحقيق المعلوماتي لأجل الوصول إلى الجاني مهما كان موقعه وتسليمه ليد العدالة للتعامل معه بشأن جرمه، إن عمل هذه الهيئات لا يؤتي أكله إلا من خلال التعاون مع أجهزة الأمن الداخلية، أي الجهات المختصة بالبحث و التحقيق على المستوى الداخلي للدول الأعضاء فيها كهيئة الأنتربول و الأوروبول و الأوروجست، ولذلك فإننا نجد أغلب الدول الغربية قد اتجهت صوب تخصيص وحدات أمنية وقضائية مختصة في مجال الجرائم المعلوماتية نذكر منها وعلى سبيل المثال لا الحصر ما هو عليه الحال في بعض التشريعات الغربية (الفرع الأول)، و التشريع الفرنسي خصوصا باعتباره عينة بحث مقارنة (الفرع الثاني).

الفرع الأول: الوحدات المختصة بمكافحة جرائم المعلوماتية في بعض الدول.

أسست أغلب الدول المتقدمة الغربية منها خصوصا وحدات خاصة بمكافحة الجرائم المعلوماتية ، كما تتولى في نفس الوقت مسائل البحث و التحقيق بشأنها نذكر منها ما هو عليه الحال في :

الفقرة الأولى : على مستوى دول شرق آسيا .

أولا : في هونغ كونغ أُسسَت وحدة خاصة تحت اسم "قوة مكافحة قرصنة الانترنت" في ديسمبر سنة 1999، و التي استطاعت في ظرف 06 أشهر من تأسيسها القبض على 12 شخصا في خمس قضايا قيد التحقيق.

ثانيا : الصين فقد تأسست و بتاريخ 2000/08/22 ما يعرف بالقوة المضادة للهاكرز، و التي تتخذ من المعهد العالي للطاقة الفيزيائية مقرا لها، وهي مختصة بمراقبة المعلومات التي يسمح لمواطنيها الدخول إليها عبر شبكة الانترنت إذ تلزم هذه الأخيرة المستخدم بتسجيل نفسه لدى مكاتب الشرطة من أجل مراقبة نشاطه عبر الشبكة.

الفقرة الثانية : على مستوى بعض الدول الأوروبية و الدول الأنجلوساكسونية.

أولا : في اسبانيا شكلت الإدارة المركزية لوزارة الداخلية الإسبانية وحدة خاصة تعرف باسم " وحدة التحريات المركزية المعنية بمعلومات جرائم الانترنت" تعمل على مراقبة النشاط الإجرامي المستحدث وملاحقة مجرمي المعلوماتية.

ثانيا : في الولايات المتحدة الأمريكية و التي ترتفع فيها معدلات الجريمة المعلوماتية و الخسائر الناتجة عنها فإنه تم إنشاء وتنصيب عدة وحدات للشرطة لأجل مواجهة هذه الجرائم منها:[1]

1 معهد أمن الحواسيب: (Computer Sécurity Institute) : هو مكتب يعمل تحت وصاية مكتب التحقيقات الفيدرالية لسان فرانسيسكو يهتم بتحقيق التكامل في الجوانب المتعلقة بالأمن المعلوماتي، ويقوم في سبيل ذلك بنشر تقارير سنوية حول مدى خطورة مسائل الأمن المعلوماتي وتنامي الجرائم المعلوماتية في نطاق الإقليم الأمريكي.

---

[1]– نبيلة هبة هروال– مرجع سابق– ص 107–108.

2 معهد شكاوي الاحتيال عبر الانترنت(Internet Fraud Complaint Center): أنشأ سنة 2001 من قبل مكتب التحقيقات الفيدرالي FBI، بالتعاون مع المكتب الأبيض الوطني لمكافحة الجرائم المعلوماتية، وهو مركز يوفر وعلى الشبكة إمكانية تقديم الشكاوى المتعلقة بالاحتيال المعلوماتي من أجل جمعها وتحليلها وتقديمها في شكل إحصائي للسلطات المختصة في سبيل توضيح بيان مدى تنامي الظاهرة الإجرامية[1].

3 وحدة جرائم الانترنت: هي وحدة مختصة بالتحقيق في جرائم المعلوماتية المتصلة بالملكية الفكرية و الجرائم المستحدثة يرأسها مساعد من مكتب التحقيقات الفيدرالي FBI، وهي بمثابة وحدة التفتيش الجنائي.

4 مكتب رئيس التكنولوجيا: وهو مكتب مفوض من قبل مكتب مدير التحقيقات الفدرالية (FBI) لتسيير مختلف المشاريع التكنولوجية الخاصة بملاحقة مرتكبي جرائم المعلوماتية كالملاحقة الشهيرة التي قان بها تحت اسم كارنيفور و المصباح العجيب.

5 المركز الوطني لحماية البنية التحتية: وهو مركز تابع للمباحث الفيدرالية الأمريكية و الذي أنشأ في 1998/02/28 بأمر من الرئيس " بيل كلينتون" بعد التقرير المقدم إليه حول حجم التهديدات التي تستهدف البنى التحتية الخاصة بنظم الاتصال وهو يعمل بالتنسيق مع وزارة الدفاع الأمريكية وهو فريق ذو طبع سري يتكون من 125 رجل حكومي مختص في أمن النظم المعلوماتية:

تعمل كل هذه الهيئات تحت تأطير مكتب التحقيقات الفيدرالي الذي يعتبر في حد ذاته الجهاز القيادي لمكافحة الجرائم المعلوماتية[2].

---

[1]–Mohamed Chawki – op cit – p 102,103.

[2]– نبيلة هبة هروال– مرجع سابق– ص 109.

ثالثا: في بريطانيا: أنشأت الفرقة الخاصة بمكافحة جرائم التقنية العالية(National Hitech Crime Unite) و ذلك في أفريل من سنة 2001، وتعتبر الفرقة الأولى المختصة مباشرة بمكافحة الجرائم المعلوماتية على المستوى المملكة المتحدة وذلك بالتعاون مع مختلف الهيئات الدولية[1].

تضم هذه الفرقة في صفوفها 80 مفتشا من رجال الشرطة و الجمارك ورجال مصلحة الاستعلامات، كلهم من أبرز المختصين في مجال البحث و التحقيق في الجرائم المعلوماتية، تتخذ ممن لندن مقرا لها يعمل على مستواها 40 مفتشا أما ال 40 الآخرون فيتوزعون على الوحدات المحلية، ويتركز عملها على ملاحقة و تتبع مجرمي المعلوماتية خصوصا الشواذ جنسيا منهم وفئة القراصنة المحترفين و المخربين ناشري الفيروسات[2].

الفرع الثاني: الوحدات المختصة بالبحث و التحقيق في جرائم المعلوماتية في التشريع الفرنسي.

يعتبر النظام الفرنسي الأقرب للنظام الجزائري من حيث وجهات النظر التشريعية و القانونية، ولذلك حاولنا في بحثنا هذا وفي هذا الفرع خصوصا التركيز حول هيكله التنظيمي في مجال سياسة مكافحة الجرائم المعلوماتية من خلال استعراض كل الهيئات المختصة بمكافحة الجرائم المعلوماتية على اختلاف انتماءاتها.

يعتبر النظام الفرنسي من الأنظمة الفاعلة، و الأكثر تطورا وتماشيا مع الجرائم المستحدثة وجرائم التقنية العالية و الجرائم المعلوماتية، من خلال تبني سياسة وإستراتيجية أمنية ذات نظرة حديثة ومتطورة في مواجهة التهديدات المعلوماتية.[3]

---

[1]–Mohamed Chawki – op cit – p 104.

[2]– نبيلة هبة هروال– مرجع سابق– ص 111.

[3] – شرعت وحدات الشرطة و الدرك الفرنسي في إجراءات مراقبة الشبكات المعلوماتية منذ سنة 1998 ، من خلال تجنيد أكثر من 120 عون للقيام بهذه المهمة ، بعد تكوينهم في مجال التحريات الخاصة بالجرائم المتصلة بالتكنولوجيات الحديثة ،

إن التوجه نحو تبني هذه الإستراتيجية كان نتاج التقرير المعنون بالكتاب الأبيض المتعلق بالأمن و الدفاع الوطني، والذي صنف الهجمات المعلوماتية ضمن خانة أخطر الجرائم التي يمكن أن تستهدف المؤسسات و الهيئات الفرنسية، وهو ما دفع بالحكومة الفرنسية إلى العمل على تقوية القدرات الخاصة في مجال الأمن المعلوماتي، من خلال اعتبار مسألة حماية النظم المعلوماتية كجزء لا يتجزأ من سياسة الدفاع و الأمن الوطني، واضعا في ذلك جدية التهديدات التي تشكلها الجريمة المعلوماتية موضع اعتبار، وهو ما تجسد من خلال إنشاء وحدات متخصصة في مجال مكافحة المعلوماتية[1].

الفقرة الأولى: الوكالة الوطنية لأمن النظم المعلوماتية

L'agence Nationale de la sécurité des systèmes

أنشأت هذه الوكالة سنة 2009 شهر جويلية، بدل المديرية المركزية لأمن النظم المعلوماتية المنشأة سنة 2001، وذلك بهدف مواجهة تنامي الجريمة المعلوماتية حسب التقرير الوارد في الكتاب الأبيض، وتعتبر هذه الوكالة وزارية فهي تخضع لمصالح الوزارة الأولى الفرنسية، تختص وعلى المستوى الوطني بإعداد واقتراح قوانين خاصة بأمن النظم المعلوماتية، كما تسهر على ضمان تطبيق النصوص حسب المعايير المحددة سلفا ، و تختص هذه الوكالة بتنفيذ المهام التالية:

و قد وضعت لذلك بدءا نظام خاص يعمل بدعم من برنامج SimAnalyst لمراقبة المعاملات الخاصة بالبطاقات الإلكترونية و تحديد الجرائم المتعلقة بها ، لتتطور الوسائل المستعملة في هذا المجال من خلال تجسيد مشروع بنك معلومات يجمع كل صور النشاطات الإجرامية الواقعة على الشبكات و بالخصوص جرائم الإستغلال الجنسي للأطفال، من خلال الإستعانة ببرامج معدة خصيصا لذلك كبرنامج Log IRC و Log P2P و هو ما سمح لها سنة 2003 بتحصيل أكثر من 600,000 ألف معلومة حول جرائم المعلوماتية . أنظر في ذلك :

Eric Filiol et Philippe Richard- Cyber Criminalité-enquête sur les mafias qui envahissent le web- Edition Dunod-paris –France- 2006-p 149,150.

[1]-Myriam Quémnéner –« La Coopération Entre les Organes de Lutte Contre la Cybercriminalité - pour une stratégie globale de cyber sécurité Français » - Article publier sur La Revue Electronique : Lamy Droits des affaires –Num- 87- France - Année 2013 - P 01.

- العمل على كشف الهجمات الإلكترونية التي تستهدف النظم المعلوماتية الحكومية.
- التصدي للهجمات الإلكترونية التي يمكن أن تستهدف النظم المعلوماتية الحكومية.
- تسيير مركز العمليات الخاص بمراقبة المواقع الحساسة للهجمات.
- العمل على الوقاية من الهجمات الإلكترونية من خلال تطوير برامج حماية أمنية ذات تقنية جد عالية.
- دعم الإدارات و المؤسسات الحيوية الفرنسية في مجال الأمن المعلوماتي.
- العمل على توعية أفراد المجتمع الفرنسي بإخطار الهجمات الإلكترونية[1].

الفقرة الثانية: المرصد الوطني لمكافحة الجرائم المتصلة بتكنولوجيا المعلومات و الاتصال.

L'office central de lutte contre la cybercriminalité liée aux technologies de l'information

(L.O.C.L.C.T.I.C)

أنشأ هذا المرصد بموجب مرسوم وزاري مشترك بتاريخ 15 ماي 2000، وهو عبارة عن هيئة مختصة وعلى صعيد كامل الإقليم الفرنسي بالمسائل المتعلقة بالجرائم المعلوماتية، وقد جاء خلفا للفرقة المركزية لقمع الجرائم المعلوماتية المنشأة سنة 1994، يعمل هذا المرصد على التنسيق وعلى المستوى الوطني من أجل وضع خطط للعمليات الموجهة ضد المجرمين المعلوماتين، وفي هذا الصدد يتولى هذا المرصد تسيير عمليات البحث و التحقيق الخاصة بجرائم المعلوماتية، كما ينفذ الأوامر الخاصة بذلك الصادرة عن الجهات القضائية المختصة، ويعتبر هذا المرصد نقطة وصل مركزية تسمح بتبادل المعلومات مع مختلف الهيئات الدولية المختصة في هذا المجال كالأنتربول[2].

---

[1]– Myriam Quémnéner –« La Coopération Entre les Organes de Lutte Contre la Cybercriminalité – pour une stratégie globale de cybersécurité Français » –op.cit – p 02

[2] – Frédérique Chopin– La Cybercriminalité– Exposé publié sur L'Encyclopédie Electronique : Le Répertoire de Droit pénal et de Procédure Pénale – juillet– 2013– paris– France– p 02.

يوفر هذا المرصد قاعدة بيانات خاصة بالتبليغ عن كافة أشال الجرائم المعلوماتية، في شكل موقع إلكتروني يحتوي على استمارة تبليغ معلوماتية ففي سنة 2008 تم تسجيل 124000 ألف تبليغ على الموقع المخصص، 1910 منها أحيلت لجهات التحقيق الخاصة بهيئة الأنتربول، و 434 منها أحيلت على جهات التحقيق القضائية الداخلية، انتهت إحداها بتوقيف شاب من ضواحي باريس فتح موقعا خاصا ببيع المخدرات و الأسلحة النارية[1].

يظم هذا المرصد 50 شرطيا ودركيا يتمتعون بالمعرفة و الخبرة في مجال النظم المعلوماتية، منحهم القانون صلاحية مباشرة الإجراءات على المستوى الوطني وهو مقسمون على الوحدات التالية:

أولا: الوحدة العملية La section Opérationnelle

تختص هذه المجموعة بالنظر في القضايا الإجرامية المتصلة بنظم المعلوماتية ذات البعد الوطني و الدولي، وتعمل على مهام الكشف عن عصابات المجرمين المعلوماتيين وتنقسم بدورها إلى خمس (05) مجموعات من المحققين المختصين هي:

- فرقة البحث و التحري في الجرائم المتعلقة ببطاقات الدفع الإلكترونية.
- فرقة البحث و التحري في جرائم الاحتيال ضد موردي خدمات الاتصال.
- فرقة البحث و التحري في الجرائم الماسة بنظم الدفع الإلكتروني.
- فرقة البحث و التحري في جرائم القرصنة الإلكترونية.
- فرقة البحث و التحري في بجرائم النصب و الاحتيال الإلكتروني[2].

---

[1]– Myriam Quéméner – Joël Ferry– Cybercriminalité Défi mondial– op.cit– p214.

[2] – Adeline Champagnat–« L'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication » Article publié sur la revue : cybercriminalité cybermenace et cyberfraude – sous la direction de : Irène Bouhadana et William Gilles – Edition– IMODEV– Paris– France–2012– p 164.

ثانيا المجموعة التقنية .La Section technique

تعمل هذه الوحدة على دعم مصالح البحث و التحقيق من خلال عملها، إضافة إلى تكوين المحققين المختصين في مجال الجرائم المعلوماتية وهي فرقة مزودة بأحدث التجهيزات من حواسيب وبرمجيات متطورة في مجال الكشف عن الدليل الإلكتروني[1].

ثالثا: وحدة تلقي وتحليل البلاغات .La section de traitement des signalements

تتكون هذه المجموعة من فرقتين:

1 فرقة (PHAROS) أنشأت يوم 06 جانفي 2009 مهمتها تسيير قاعدة البيانات الخاصة بجمع وتحليل المهام على الجهات المختصة سواء الفرنسية منها أو الدولية، من أجل البحث و التحقيق بشأن الجرائم المبلغ عنها، من خلال موقعها الإلكتروني على الرابط www.internet-signalement.gouv.fr.

2 فرقة (Info. Escroqueries) : تهتم بالعمل في مجال تلقي المعلومات و البلاغات عبر خط هاتفي من خلال الرقم (17-02-02-11-8-33+) وهو مخصص للضحايا في مجال الاحتيال الإلكتروني، وقد تلقت هذه الفرقة سنة 2010 حوالي 23695 اتصالا يحمل شكاوى من ضحايا وقعوا في شرك الاحتيال.

رابعا: وحدة العلاقات الدولية

تعمل هذه الوحدة على ربط الاتصالات مع مختلف المصالح التي تعمل بالاشتراك مع المرصد، إضافة إلى كونها نقطة اتصال مع شبكة I24/7 و I.Link الخاصة بالأنتربول[2].

---

[1]– Adeline Champagnat– op–cit– p 166.

[2] – Ibid– p 167 ,168.

الفقرة الثالثة: الجهات التابعة لمصالح الشرطة الفرنسية.

تتعدد المصالح المختصة بالبحث و التحقيق في مجال الجرائم المعلوماتية و التي تخضع لإدارة الجهاز الأمني الفرنسي إلى:

أولا: فرقة البحث و التحري عن جرائم الغش المعلوماتي.

.La Brigade d'enquêtes sur les fraudes aux technologies de l'information (B.E.F.T.I)

تضم هذه الفرقة العملية حوالي 30 شرطيا في صفوفها، يعملون تحت سلطة محافظة شرطة باريس، يختص أفرادها بمهمة البحث و التحقيق في الجرائم المعلوماتية، وكذلك بدعم أي جهة أخرى تتولى مسألة البحث و التحقيق في المسائل الإلكترونية، كما تضمن التكفل بمهمة التكوين و التوعية لمصالح الشرطة الأخرى، تختص هذه الفرقة إقليما بحدود مدينة باريس ويمكن تمديد اختصاصها إلى كامل الإقليم الفرنسي ، وتنقسم هذه الفرقة إلى ثلاث خلايا عملية[1]:

- خلية البحث و التحقيق.
- خلية المبادرة.
- خلية الدعم

وتتبنى كهدف أساسي إلى مكافحة جرائم المعلوماتية الماسة بالتقليد في البرمجيات، و الاعتداء على حقوق المؤلف و الغير، إضافة إلى باقي الجرائم الأخرى المرتكبة عبر شبكة الانترنت، وخصوصا الاستغلال الجنسي للأطفال عبر الشبكة[2].

---

[1]– Myriam Quéméner – Joël Ferry– Cybercriminalité Défi mondial– op.cit– p 189.

[2]– Frédérique Chopin – op.cit– p 01.

ثانيا: فرقة مكافحة جرائم الغش المتعلقة بوسائل الدفع الإلكتروني.

Brigade des fraudes liée aux moyens de paiement (B.F.M.D)

هي فرقة تابعة وخاضعة لمحافظة شرطة باريس، لها اختصاص محلي بمدينة باريس وضواحيها، تضم في صفوفها 50 شرطيا مختص بالبحث و التحقيق في الجرائم الحديثة المتعلقة بوسائل الدفع الإلكترونية، كجرائم بطاقات الائتمان، و الاحتيال المالي[1].

ثالثا: المديرية العامة للاستخبارات الداخلية.

La Direction centrale du renseignement intérieur (D.C.R.I)

تهتم هذه الهيئة بالوقاية وقمع الجرائم على مستوى كامل التراب الفرنسي ، و تلك التي تنشأ أو تكون مدعومة من قبل قوى خارجية أجنبية، و التي من شأنها الإضرار بأمن البلاد و المصالح الأساسية، وهي تهتم بمكافحة الجرائم المعلوماتية كالتجسس المعلوماتي من قبل دولة أجنبية، و التخطيط لتنفيذ أعمال إرهابية[2].

الفقرة الرابعة: الوحدات الخاصة بالدرك الفرنسي.

يخضع لاختصاص جهة الدرك الفرنسي، فرق ووحدات مختصة في مجال مكافحة الجرائم المعلوماتية من خلال اختصاصها بالبحث و التحقيق بشأنها وهي:

أولا: معهد البحث الجنائي للدرك الوطني:

L'institut de Recherche Criminelles de la Gendarmerie National (I.R.C.G.N)

يخضع هذا المعهد للإدارة العامة للدرك الفرنسي له أربع (04) مهام:

---

[1]– Myriam Quéméner– Jean Paul Pinte – Cyber sécurité– op.cit– p190.

[2]–Myriam Quémnéner – « La Coopération Entre les Organes de Lutte Contre la Cybercriminalité – pour une stratégie globale de cybersécurité Français » – op.cit – p 02.

- تنفيذ طلبات الوحدات الخاصة و القضاء من أجل انجاز تقارير خبرة علمية ضرورية لأجل تسيير التحقيقات القضائية.
- تقديم يد العون للمحققين الميدانيين.
- تكوين المختصين في مجال التحقيق الجنائي.
- البحث في مجال تطوير وسائل التحقيق الجنائي[1].

ثانيا: وحدة المعلوماتية و الإلكترونيات: هي وحدة تابعة لمعهد البحث الجنائي السالف الذكر، يختص بالتحقيق في القضايا ذات الطابع العلمي، ومن مهامها الأساسية إجراء التحقيقات المتعلقة "بالأدلة العلمية"، تلعب هذه الوحدة دورا جوهريا في التحقيق الجنائي، نظرا لتركيبتها فهي تضم خيرة خبراء التحقيق الجنائي في مجال جمع الأدلة، وتحليلها وتقوم بالمهام التالية:

- تنفيذ أوامر ضابط الشرطة القضائية و القضاة بشأن معاينة مسرح الجريمة
- تقديم يد العون في حالة الجرائم المعقدة و تأطير وتكوين خبراء التحقيق الجنائي.
- البحث في ميدان علم الأدلة الجنائية[2].

ثالثا: الفرقة التقنية للبحث القضائي و التوثيق.

Le service technique de recherche judiciaire et de documentation.

تختص هذه الغرفة وعلى مستوى كامل الإقليم الفرنسي، بمهمة تجميع وتحليل بطريقة عملية وبأهداف إستراتيجية، كل المعلومات المتوفرة حول الجرائم، و التي توفرها الجهات التابعة للشرطة القضائية أو تلك الناجمة عن التحقيقات التي تباشرها وحدات الدرك الوطني بشأن الجرائم المصنفة كجنايات وجنح[3].

---

[1] – Frédérique Chopin– op.cit –p 01.

[2] – Céline Renard Castétes– op.cit – p 538.

[3]–Myriam Quéméner – Joël Ferry – Cybercriminalité Défi mondial– op.cit– p 219.

كما تعمل كذلك على إدارة المعلومات القضائية من خلال ضمان تسيير قاعدة البيانات الخاصة بذلك ، وانجاز التحقيقات القضائية من خلال عمل الغرفة الإقليمية للاستعلامات.[1]

أوكلت لهذه الغرفة مهام أساسية متعلقة بالبحث و التحقيق في الجرائم المعلوماتية وذلك سنة 1998 وهو ما نتج عنه خلق ثلاث وحدات فرعية هي:

- وحدة قمع الجرائم الماسة بالقصر عبر شبكة الانترنت (RAMI)
- وحدة التحقيقات بشأن جرائم الانترنت (D2I).
- وحدة الدعم و الإسناد .[2]

تتمتع هذه الوحدات باختصاص إقليمي وطني، في مجال أعمال البحث و التحقيق بشأن الجرائم المعلوماتية، وتستعين في عملها بدعم وإسناد مركز المراقبة التقني الموجود بضواحي (روسني سوبوا) (Rosny- Sous bois) تضم مجموعة من المحققين المختصين في المجال تحت اسم (N .T.E.C.H) ينفذون بناء على طلبات وحدات الدرك الوطني أو القضاة كل مهام البحث و التحقيق من إعداد تقارير، ودعم مادي وتقني في مجال الجرائم المعلوماتية.[3]

الفرع الثالث: دور الجمارك الفرنسية في أعمال البحث و التحقيق المعلوماتي.

تعتبر الجمارك هيئة إدارية ضريبية تلعب دورا رئيسيا يبرز من خلال:

---

[1]-Myriam Quéméner- Jean Paul Pinte - Cyber sécurité- op.cit- p 190.

[2]-Myriam Quémnéner -« La Coopération Entre les Organes de Lutte Contre la Cybercriminalité - pour une stratégie globale de cybersécurité Français » - op.cit - p 03.

[3]-Myriam Quéménér- Jean Paul Pinte - Cyber sécurité- op.cit- p 192.

- لعب دور ضريبي من حيث تمويل الخزينة العمومية بما مقداره 13% من الدخل الوطني.
- لعب دور اقتصادي ورقابي يتمل في ضمان أمن وسيولة تنقل البضائع.
- لعب دور مكافحة الجرائم الجمركية و الغش الجمركي على المستوى الدولي ضمانا لمصالح الدولة الداخلية.[1]

كما تلعب الجمارك و في ظل المتغيرات الحديثة ، و في ظل إستهداف الجرائم المعلوماتية للجانب الإقتصادي بالضرر ، دورا مهما في أعمال البحث و التحقيق في الجرائم المعلوماتية ، من خلال منحها سلطات قضائية في ذلك ، و دعمها بوسائل و أساليب لأجل تحقيق ذلك .

الفقرة الأولى : إختصاص وحدات الجمارك الفرنسية بأعمال البحث و التحقيق في الجرائم المعلوماتية.

تتدخل مصالح الجمارك في مجال مكافحة الجرائم المعلوماتية من خلال استعمال حقها في حجز البضائع المقلدة على مستوى مخازن البريد ومخازن التوصيل على السريع، التي تعتبر أفضل مكان يلجأ إليه المقلدون لإرسال سلعهم المباعة عبر شبكة الانترنت، و التي شكلت نسبة 11% سنة 2011 من مجموع السلع المقلدة، لتصل إلى 30% سنة 2012 وهو ما يفسر حجم التنامي الخطير لأخطار شبكة الانترنت على صحة الاقتصاد الفرنسي[2].

وفي ظل هذه الأوضاع و التي كانت متوقعة مسبقا، فقد تقرر وبتاريخ 1999/06/23 إسناد مهام قضائية لإدارة الجمارك بهدف تدعيم فعالية الإجراءات الجنائية، فأصبح بمقدور بعض أعوان الجمارك المختصين و المؤهلين مباشرة متابعات قضائية بموجب طلب من وكيل الجمهورية أو قاضي التحقيق، وقد

---

[1]–Myriam Quéméner – Joël Ferry– Cybercriminalité Défi mondial– op.cit– p 219.

[2]–Myriam Quémnéner –« La Coopération Entre les Organes de Lutte Contre la Cybercriminalité – pour une stratégie globale de cybersécurité Français » –op.cit – p 03.

تدعم ذلك بصدور القرار المؤرخ في 2002/12/05 المتضمن إنشاء الإدارة المركزية للجمارك القضائية، التي تضم أعوان جمارك مؤهلين يصطلح عليهم " ضباط الجمارك القضائية"، وهو مرفق يعمل وفق مبدأ الاختصاص الوطني تابع للمديرية العامة للجمارك الفرنسية، يسير من قبل قاضي التحقيق، وقد تدعم عمل واختصاصات هذه الهيئة بصدور قانون (PER BEN 2) في 04 مارس 2004، المتعلق بضرورة تطوير مرفق العدالة وفق تطور الجريمة، وهو ما سمح لهذه الجهة بممارسة أعمالها ضمن نطاق حرية أوسع في مجال محاربة الجريمة المنظمة، غير أن تاريخ فيفري 2009، وما حمل معه من قرار بإنشاء "خلية الجمارك المعلوماتية" شكل نقطة تحول في عمل و إختصاص هذه الفئة بدخولها بصفة علنية عالم البحث و التحقيق في الجرائم المعلوماتية، من خلال دعم عمل هذه الخلية بنصوص قانونية ووسائل مادية تسمح لها بمزاولة عملها، بتتبع المواقع الإلكترونية المشبوهة في مجال الصفقات غير المشروعة عبر الانترنت، وهو ما مكنها بالإطاحة بشبكة دولية مختصة بتقليد المنتجات القادمة من الصين وبيعها بأوروبا و التي جنى أفرادها ما يقارب 4.6 مليون أورو، تم تبييضها بسويسرا، وذلك من خلال إتباع أساليب خاصة نستعرضها في التالي:

الفقرة الثانية: أساليب إدارة الجمارك في البحث و التحقيق بشأن الجرائم المعلوماتية.

تباشر خلية الجمارك المعلوماتية سلطتها في مواجهة الجريمة المعلوماتية من خلال إتباع الأساليب التالية:

أولا: أسلوب استفزاز عمليات الشراء عبر شبكة الانترنت.

يسمح القانون لخلية الجمارك المعلوماتية بمراقبة عمليات التبادل الإلكتروني للسلع و المنتجات وكذلك يسمح لهم بالقيام بعمليات شراء مباشرة من المواقع محل المراقبة وذلك بهدف تحديد طبيعة المنتوج المقلد أو المحظور و الوصول إلى بائعه وتحديد مسار الدفع الإلكتروني.

ثانيا: أسلوب التسرب ضمن مواقع القمار الإلكترونية.

بموجب قانون 12 ماي 2010 منح الحق لضباط الجمارك القضائية للمشاركة في ألعاب القمار عبر الانترنت وذلك تحت أسماء مستعارة، بهدف كشف عمليات تبيض الأموال و الاحتيال الالكتروني و كل الجرائم لمتصلة بذلك.

ثالثا: أسلوب الاتصال بالغير.

يحق لضباط الجمارك القضائية الاتصال بأي خص يحوز على وثائق أو معلومات من شأنها إفادة مصلحة الجمارك بمعلومات حول نشاطات غير مشروعة ، و تعمل خلية الجمارك المعلوماتية وفق منهجية ثلاثية القواعد هي: جمع المعلومات حول المتهم، تحديد مسار البضاعة محل الجريمة، تحديد مسار أموال الدفع الإلكتروني[1].

إذن يعتبر النظام الفرنسي وفي مجال مواجهة الجرائم المعلوماتية ومسائل البحث و التحقيق بشأنها من الأنشطة الفعالة و الرائدة في هذا المجال، بحكم تعدد وتنوع الوحدات و الهيئات المختصة بهذه المهام من وزارية و أمنية وهو النظام الذي يحاول التشريع و التنظيم الجزائري الإقتداء به من خلال ما سنستعرضه في المطلب الثالث من هذا المبحث.

المطلب الثالث : الوحدات المختصة بتولي اجراءات البحث و التحقيق في الجرائم المعلوماتية على المستوى الوطني .

يختص على المستوى الوطني بمهام مباشرة أعمال البحث و التحقيق في الجرائم المعلوماتية وحدات متخصصة منها التابعة لوزارة العدل ، و أخرى تابعة لسلك الأمن الوطني ، و منها ما هي تابعة لسلك الدرك الوطني ، و هي وحدات أغلبها حديثة النشأة نظرا لحداثة المجتمع الجزائري مع عهد الجرائم المعلوماتية ، و التي تعرف إنتشارا متزايدا تماشيا و إنتشار تكنولوجيا المعلومات المرتبطة أساسا بإستعمال الحواسيب و شبكة الانترنت ،و كذلك الهواتف الذكية المرتبطة بشبكة الأنترنت للجيل الثالث .

---

[1] – Gérard Schoen –« La douane face a la cybercriminalité »– Article publié sur la revue : cybercriminalité cybermenace et cyberfraude – sous la direction de : Irène Bouhadana et William Gilles – Edition– IMODEV– Paris– France–2012– p 169–170.

و سنحاول من خلال هذا المطلب إستعراض أبرز الهيئات و الوحدات المتخصصة في مجال مكافحة الجرائم المعلوماتية ، و التي ما تسند إليها عادة مهام الوقاية و مكافحة الجرائم المعلوماتية ، نظرا لتشكيلتها البشرية الخاصة و التي تضم محققين من نوع خاص تجتمع لديهم صفة ضابط شرطة قضائية إضافة إلى المعرفة الواسعة بمجال النظم المعلوماتية و الإجرام المعلوماتي ، مما يسمح لهم و يؤهلهم لتولي مهام البحث و التحقيق في ميدان الجرائم المعلوماتية بدل الجهات القضائية، سواء تمثلت في شخص وكيل الجمهورية او قاضي التحقيق نظرا لقلة خبرتهم بميدان النظم المعلوماتية و عدم تحكمهم في تقنيات البحث و التحقيق بواسطة وسائل معلوماتية خاصة تتطلب المعرفة و الدقة في مجال إستخدامها ، و لعل أن أبرز هذه الهيئات و الوحدات هي الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال (الفرع الأول) ، إضافة إلى تلك الوحدات التابعة لسلك الأمن الوطني (الفرع الثاني)، و كذلك تلك التابعة لقيادة الدرك الوطني (الفرع الثالث) .

الفرع الأول : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال.

تعود فكرة إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال إلى سنة 2009 و بالضبط منذ تاريخ 05 أوت 2009 تاريخ صدور القانون 09-04 المتعلق بتحديد القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ، بحيث جاء في نص المادة 13 من القانون على انه تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحته ، تحدد تشكيلة الهيئة و تنظيمها و كيفية سيرها عن طريق التنظيم .

و قد إستلزم الأمر لصدور التنظيم الذي طرحته نص المادة 13 السالفة الذكر الإنتظار لمدة 06 سنوات كاملة ، أين صدر المرسوم الرئاسي رقم 15-268 بتاريخ 08 أكتوبر 2015 ضمن العدد الثالث

و الخمسين 53 للجريدة الرسمية ، و الذي تضمن في فصوله تحديد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها. [1]

الفقرة الأولى : التعريف بالهيئة و إختصاصاتها .

أولا : التعريف بالهيئة : تعتبر " الهيئة " كما يصطلح عليها في صلب نصوص المرسوم الرئاسي حسب أحكام المواد من 01 إلى 04 منه بأنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية و الإستقلال المالي توضع لدى الوزير المكلف بالعدل ، و يقع مقرها بالجزائر العاصمة، تتولى الهيئة المهام المنصوص عليها في المادة 14 من القانون 09-04 و ذلك تحت رقابة السلطة القضائية و طبقا لأحكام قانون الإجراءات الجزائية. [2]

ثانيا : إختصاصات الهيئة : بينت الفقرة الثانية 02 من المادة 04 من المرسوم الرئاسي 15-261 المهام الأساسية التي تكلف بها الهيئة و هي و على سبيل الحصر مهام الهدف منها هو الوقاية من الجرائم المعلوماتية ، و مكافحة هذه الأخيرة من خلال الإسهام في أعمال البحث و التحقيق و مد يد العون لمصالح الشرطة القضائية و أبرز مهام هذه الهيئة هي :

---

[1] – لمزيد من التفصيل انظر الملحق رقم : **03**

[2] – تنص المادة 14 من قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال على انه " تتولى الهيئة المذكورة في المادة 13 خصوصا المهام التالية :

أ– تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحته.

ب– مساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال، بما في ذلك تجميع المعلومات و ‘نجاز الخبرات القضائية.

ج– تبادل المعلومات مع نظيرتها في الخارج قصد جمع المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و تحديد مكان تواجدهم.

1- إقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال .

2- تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحته.

3- مساعدة السلطات القضائية و مصالح الشرطة القضائية في مجال مكافحة الجرائم المعلوماتية من خلال مدها بالمعلومات و الخبرات القضائية,

4- ضمان المراقبة الوقائية للإتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية و التخريبية و الماسة بأمن الدولة و ذلك تحت سلطة قاضي مختص و و ذلك كإختصاص حصري .

5- تجميع و تسجيل و حفظ المعطيات الرقمية و تحديد مسارها من أجل إستعمالها في الإجراءات القضائية.

6- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا المعلومات

7- تطوير التعاون مع المؤسسات و الهيئات الوطنية المعنية بالجرائم المعلوماتية.

8- تنفيذ الطلبات الصادرة عن الدول الأجنبية و تطوير سبل التعاون و التبادل معها.

9- المساهمة في تحديث المعايير القانونية في مجال إختصاصها .

الفقرة الثانية : تشكيلة الهيئة و طبيعة عملها .

اولا : تشكيلة الهيئة الإدارية : تتشكل الهيئة من لجنة مديرة إضافة إلى مديرية عامة ، تتشكل اللجنة المديرة من الوزير المكلف بالعدل رئيسا إضافة إلى الوزير المكلف بالداخلية و الوزير المكلف بتكنولوجيات الإعلام و الإتصال و قائد الدرك الوطني و كذلك المدير العام للأمن الوطني ، و ممثلين أحدهما عن رئاسة الجمهورية و الأخر عن وزارة الدفاع يكملها قاضيان من المحكمة العليا ، اما المديرية العامة فيرأسها مدير عام يعين بموجب مرسوم رئاسي ، و تتجلى مهام هذه المديريات في ضبط برامج عمل الهيئة

و دراسة مشروع الميزانية و تقديم تقارير خاصة بنشاط الهيئة، و بالتالي فهي لا تسهم في الإجراءات الخاصة بالوقاية او بمكافحة الجرائم المعلوماتية .[1]

ثانيا : تشكيلة الهيئة التقنية : إضافة إلى اللجان الإدارية تضم الهيئة مديريات تتسم من حيث مهامها و تشكليتها بالطابع التقني، بإعتبارها المختصة بإنجاز المهام التقنية المتعلقة بالوقاية و وبمكافحة الجرائم المعلوماتية و هذه المديريات هي :

1 – مديرية المراقبة الوقائية و اليقظة الإلكترونية : لم يشر الأمر الرئاسي 15-261 إلى تشكيلة هذه المديرية ،غير أنه و من خلال تحليل نص المادة 18 منه يمكن لنا تحديد تشكيلتها في مجموعة من ضباط و اعوان الشرطة القضائية المختصين في مجال مكافحة الجرائم المعلوماتية، من سلك الأمن الوطني و كذلك الدرك الوطني و المصالح العسكرية للإستعلام و الأمن، يعينون بموجب قرارات مشتركة بين الوزراء المكلفين بالعدل و الدفاع و الداخلية ، يساعدهم مستخدمي الدعم التقني و الإداري من نفس الأسلاك .

تعمل هذه المديرية على إنجاز المهام التالية :

1- تنفيذ عمليات المراقبة الوقائية للإتصالات الإلكترونية و القيام بإجراءات التفتيش و الحجز داخل الأنظمة المعلوماتية إذا ما تعلق الأمر جرائم الإرهاب او التخريب و الجرائم الماسة بأمن الدولة بناء على رخصة مكتوبة من السلطة القضائية و تحت رقابة القاضي المختص.[2]

---

[1] – المادة 06-07-08-09-10 من المرسوم الرئاسي 15-261 الذي يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها.

[2] – يعتبر هذا الإجراء تكليفا حصريا للهيئة بموجب نص المادتين 21 و 42 من المرسوم الرئاسي 15-261 الذي يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها،

2- إرسال المعلومات المحصل عليها إلى السلطات القضائية و مصالح الشرطة القضائية.

3- تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة و جمع المعطيات التي تسمح بتحديد مكان تواجد مرتكبي الجرائم المعلوماتية و التعرف عليهم .

4- جمع و مركزة كل المعلومات و إستغلالها من اجل الكشف عن الجرائم المعلوماتية.

5- المشاركة في حملات التوعية حول مخاطر تكنولوجيا الإعلام و الإتصال.

6- تزويد السلطات القضائية و مصالح الشرطة القضائية تلقائيا أو بناء على طلبها بالمعلومات و المعطيات المتعلقة بالجرائم المعلوماتية.

إذن و بالنظر إلى تشكيلة و المهام الملحقة بهذه المديرية فإنه يمكن وصفها بأنها المركز العملياتي للهيئة بما أنها تتولى الجانب التقني الخاص بإنجاز الأعمال المتعلقة بالبحث و التحقيق في الجرائم المعلوماتية ، و لعل ان ما يزيد من دورها الفعال هو تنصيبها على رأس مركز العمليات التقنية و كذلك الملحقات مما يبرز دورها الفعال في تسيير و تأطير الأعمال المتعلقة بالوقاية او بمكافحة الجرائم المعلوماتية[1] .

2 – مديرية التنسيق التقني : لم ينص المرسوم الرئاسي 15-261 على تشكيلة مديرية التنسيق التقني مما يترك المجال للقول بأنها تشكيلتها تكون بناء على قرارات مشتركة بين وزراء العدل و الدفاع و الداخلية على شاكلة مديرية المراقبة الوقائية و اليقظة الإلكترونية ، غير انها تختلف عنه من حيث المهام الموكلة إليها ، فتتمثل مهامها أكثر في الدور الوقائي و الإعلامي من خلال توليها :

و بالتالي لا يجوز إتخاذ أي إجراء في مواجهة الجرائم المعلوماتية الإرهابية أو ذات الطابع التخريبي أو الماسة بأمن الدولة من قبل أي جهة أخرى سواء امنية كانت او قضائية ، و تحول كل عمليات المراقبة الإلكترونية التي كانت تمارسها في السابق هيئات وطنية أخرى إلى إختصاص الهيئة .

[1] – المواد11-13-14- 18-21 من المرسوم الرئاسي 15-261 الذي يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها.

1- إنجاز الخبرات القضائية في مجال إختصاص الهيئة.

2- تكوين قاعدة معطيات تحليلية للإجرام المعلوماتي .

3- إعداد الإحصائيات الوطنية للإجرام المعلوماتي.

4- تسيير المنظومة المعلوماتية و إدارتها.[1]

إذن فمن خلال إستعراض الهيكل العام للهيئة و مجمل إختصاصاتها، يتضح لنا جليا مدى إقتناع الهيئة التشريعية بضرورة تفعيل دور الهيئة في مجال الوقاية و مكافحة الجرائم المعلوماتية و لو بشكل متاخر، نظرا لتوسع تطبيقات تقنية المعلوماتية في المجتمع الجزائري على الصعيدين الحكومي و الإجتماعي، و هو ما ينبئ بتنامي الإجرام المعلوماتي و إزدياد حجم التهديدات التي يشكلها على سلامة الأنظمة المعلوماتية و امن المعطيات المخزنة و المتداولة عبرها .

الفرع الثاني : الوحدات التابعة لسلك الأمن الوطني .

تضع مديرية الأمن الوطني في إطار تجسيد سياسة أمنية فعالة ، كافة الإمكانيات البشرية و التقنية المتاحة لديها لأجل التصدي لكل أنواع الجرائم و بالخصوص تلك المستحدثة منها كالجرائم المعلوماتية، و التي تعتبر نتاج التطور الحاصل على المستوى الدولي و الوطني في مجال تكنولوجيات الإعلام و الإتصال ، و ذلك بهدف حماية المصلحة العامة و كذلك المصالح الخاصة المرتبطة بإستعمال هذا النوع من التكنولوجيات .

---

[1] - المادة 12 من المرسوم الرئاسي 15-261 الذي يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها.

الفقرة الأولى : على مستوى المديرية العامة.

بادرت المديرية العامة للأمن الوطني إلى تحديث بنيتها الهيكلية بغية خلق وحدات متخصصة تعمل كل منها على مكافحة نوع معين من الجرائم دون سواها ، و لذلك قامت المديرية العامة للشرطة القضائية بإستحداث أربع 04 مصالح مختصة في شكل نيابة مديرية و هي :

1- نيابة مديرية الشرطة العلمية .

2- نيابة مديرية الإقتصادية و المالية .

3- نيابة القضايا الجنائية .

4- مصلحة البحث و التحليل.

و فيما يتعلق بمكافحة الجريمة المعلوماتية فقد أسندت المهمة لنيابة مديرية الشرطة العلمية و التقنية ، هذه الأخيرة التي تضع لخدمة هذا الهدف مصالح عملية مختصة بذلك ، تتولى أعمال البحث و التحري و التحقيق بشأن الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ، و هذه الوحدات هي :

1. المخبر المركزي للشرطة العلمية و الكائن مقره بالجزائر العاصمة.
2. المخبر الجهوي للشرطة العلمية –قسنطينة.
3. المخبر الجهوي للشرطة العلمية – وهران .

بالإضافة إلى ثلاث 03 مخابر أخرى قيد الإنجاز على مستوى – ورقلة – بشار – تمنراست ينتظر تسليمها قريبا لأجل تعميم هذا النوع من النشاط على كافة ربوع الوطن .[1]

[1]– في سبيل تدعيم المصالح الولائية للشرطة القضائية في مجال مكافحة الجرائم المعلوماتية ،خلقت المديرية العامة للأمن الوطني سنة 2010 ما يقارب 25 خلية لمكافحة الجرائم المعلوماتية موزعة على النحو التالي : 8 خلايا على مستوى الشرق، 8 خلايا على مستوى ولايات الوسط ، 6 خلايا على مستوى ولايات الغرب، 1 خلية على مستوى ولايات الجنوب

يتولى كل مخبر سواء المركزي أو الجهوي لولاية قسنطينة أو وهران ، مهام البحث و التحقيق و تحليل الأدلة الجنائية بمختلف أنواعها ، و لأجل ذلك يضم كل مخبر دائرتين هما :

الدائرة العلمية تتولى أعمال البحث و التحقيق و تحليل الأدلة المتصلة بالمجال البيولوجي و الطب الشرعي و الكيمياء و المخدرات ، و كذلك تلك المتعلقة بمجال التسميم و الحريق و المتفجرات ، كل منها على مستوى مخبر خاص.

الدائرة التقنية و تتولى مهام البحث و التحقيق و تحليل الأدلة الجنائية الناتجة عن الجرائم التي تستعمل فيها الأسلحة و القذائف بمختلف أنواعها، و كذلك جرائم التزوير، إضافة إلى الجرائم المعلوماتية، و تباشر الإجراءات الخاصة بكل جريمة على مستوى دائرة مستقلة عن الآخرى .[1]

لتقوم بعدها المديرية العامة بتعميم الخلايا هذه على جميع أمن ولايات الوطن، تعمل على رصد و كشف هذا النوع من الجرائم و تحويل مسائل البحث و التحقيق المعقدة تقنيا بشأنها إلى المخابر المركزية و الجهوية للشرطة العلمية ، و قد أحصت المديرية العامة للأمن الوطني في الـ 10 أشهر الأولى من سنة 2015 مايقارب 410 قضية معالجة تورط فيها 347 شخص . أنظر في ذلك : عبد الرحمان حملاوي– دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية– بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة– 16و 17 نوفمبر 2015– كلية الحقوق – جامعة بسكرة– الجزائر ص9،10

[1] – مساهمة المخبر الجهوي للشرطة العلمية بقسنطينة في إدارة الدليل ضمن التقنيات الخاصة للتحقيق – وثيقة خاصة صادرة عن المخبر الجهوي للشرطة العلمية – قسنطينة – نيابة مديرية الشرطة العلمية و التقنية– مديرية الشرطة القضائية– المديرية العامة للأمن الوطني– ص 02–03.

الفقرة الثانية :على المستوى الجهوي– دائرة الأدلة الرقمية و الآثار التكنولوجية التابعة لمخبر الأدلة الجنائية-قسنطينة– دراسة ميدانية.

يضم المخبر الجهوي للشرطة العلمية على مستوى ولاية قسنطينة كما هو الحال بالنسبة لمخبر ولاية وهران ، مخبرا خاصا بتولي أعمال البحث و التحقيق القائمة بشأن الجرائم المعلوماتية ، و ذلك تحت تسمية "**دائرة الأدلة الرقمية و الأثار التكنولوجية**" و التي لم تكن عند إستحداثها سنة 2004 سوى قسم ، غير أن الإرتفاع الملحوظ لعدد القضايا الناتجة عن الجرائم المعلوماتية ، بسبب الإنتشار المتزايد لتقنية المعلوماتية عجل بترقيتها إلى دائرة تضم ثلاث 03 أقسام فرعية هي :

1. **قسم إستغلال الأدلة الرقمية الناتجة عن الحواسيب و الشبكات .**
2. **قسم إستغلال الأدلة الناتجة عن الهواتف النقالة.**
3. **قسم تحليل الأصوات (ينشط هذا القسم على مستوى المخبر المركزي بالجزائر العاصمة).**

تضم الدائرة في صفوفها ثمانية 08 أعضاء محققين أربع 04 منهم أعوان شرطيون رسميون يتمتعون بصفة ضابط شرطة قضائية ، و البقية هم أعوان شبيهون، يحمل كل منهم شهادة جامعية في تخصص الإعلام الآلي ، إضافة إلى إلمامهم بالجانب القانوني ، و مما يزيد من فعاليتهم في مجال مباشرتهم لمختلف إجراءات البحث و التحقيق في الجرائم المعلوماتية هو خضوعهم بصفة دورية لدورات تكوينية لأجل الإطلاع على كل المستجدات القانونية منها و التقنية في مجال الإجرام المعلوماتي.[1]

---

[1] – ملخص الزيارة الميدانية لدائرة الأدلة الرقمية و الآثار التكنولوجية – المخبر الجهوي للشرطة العلمية لولاية قسنطينة بتاريخ : 01 أفريل 2015.

و من مهام هذا المخبر ضمان الدعم التقني لمختلف مصالح الشرطة و الأجهزة القضائية في مجال التحريات الالكترونية ، و ذلك من خلال القيام بعمليات البحث عن المعطيات المشبوهة و المعلومات الرقمية على مختلف أشكالها : ملفات، رسائل الكترونية، برامج، صور،... هذا البحث يتم عن طريق استعمال برامج و وسائل خاصة تمكن من استرجاع كل المعطيات المحذوفة، و الإطلاع على محتوى كل الوسائط الرقمية. [1]

تلعب الدائرة دورا مهما للغاية في الكشف عن أسرار الجرائم المعلوماتية ، من خلال مختلف الإجراءات التي تباشرها إما أثناء مرحلة البحث و الإستدلال ، أو أثناء مرحلة التحقيق القضائي .

فأما أثناء مرحلة البحث و التحري فإن أعضاء الدائرة عادة ما يستجيبون للطلبات التي يقدمها لهم أعوان الشرطة التابعون لخلايا مكافحة الجرائم المعلوماتية الموزعة على كل مديريات الأمن الوطني، أو لطلبات وكيل الجمهورية أو قاضي التحقيق التي تردهم في شكل إنابة قضائية ، من أجل دعمهم و مساعدتهم اثناء مرحلة المعاينة لمسرح الجريمة و كذلك لحجز الأدلة المتواجدة عليها.

أما أثناء مرحلة التحقيق القضائي فإن دور الدائرة لا يتعدى لأن يكون دور خبير ، و ذلك من خلال إعداد تقارير خبرة بناء على طلبات وكيل الجمهورية و بالخصوص قاضي التحقيق ، كنتيجة لقيام المحققين بأعمال تحليل الأدلة المحجوزة و العمل على إستخراج الأدلة الإلكترونية منها ، كتحليل محتوى الأقراص الصلبة للحواسيب المستعملة في الجريمة ، أو حواسيب الضحايا ، و كذلك كل دعامات التخزين الإلكترونية بمختلف أنواعها و أشكالها ، و كذلك المواقع التي تم إختراقها و إستهدافها وصولا إلى تحديد المواقع الجغرافي و عناوين المجرمين ، و ذلك بالإستعانة بوسائل مادية خاصة منها حواسيب متطورة ذات

---

[1] – مساهمة الشرطة العلمية و التقنية في مجال التحقيقات الجنائية– وثيقة خاصة صادرة عن مديرية الشرطة القضائية– المديرية العامة للأمن الوطني– ص 46.

جودة عالية ، إضافة إلى أجهزة أخرى كجهاز Right Blocker الذي يسمح بنسخ المعطيات من ذاكرة التخزين مهما كان نوعها ، و عمل نسخة طبق الأصل عنها من أجل العمل عليها بالتحليل و ذلك حفاظا على النسخة الأصلية من أي تحريف أو فقدان ، إضافة إلى وسائل برمجية أخرى تتمثل في برامج التتبع الإلكتروني لتحديد موقع الهجوم ، أو برامج إعادة بناء المعلومات بعد حذفها أو تخريبها ، و هي كلها برامج خاصة موضوعة تحت تصرف أعضاء الدائرة لخدمة أعمال البحث و التحقيق عن الأدلة الإلكترونية ، التي عادة ما تختتم بإعداد تقارير خبرة تقدم لقضاة التحقيق أو لقضاة الحكم في أبسط شكل ممكن حتى يتم إستيعاب مضمونها و الإستناد عليها لتسبيب الأحكام و القرارات .[1]

و بالرجوع إلى المعطيات الإحصائية المقدمة فإن سنة 2014 شهدت ما يقارب 250 قضية محل تحقيق من قبل أعضاء الدائرة ، أبرزها قضيتان وردتا على سبيل الإنابة القضائية الدولية و بالتحديد عن طريق مكتب الأنتربول تتعلق كلاهما بقيام شابين من ولاية قسنطينة بالإعتداء على الأنظمة المعلوماتية الخاصة بموقع وزارة الخارجية الكويتية و تعطيله ، و كذلك القيام بجريمة إحتيال إلكتروني على أهداف بالولايات المتحدة الأمريكية، أما فيما يخص الثلاثي الأول لسنة 2015 فإنه تم تسجيل 60 قضية طرحت أمام محققي دائرة الأدلة الرقمية و الأثار التكنولوجية للنظر فيها ، تتعلق أغلبها بسوء إستخدام مواقع التواصل الإجتماعي من خلال قضايا المساس بالأشخاص في صورة الإبتزاز و القذف و التشهير .[2]

و في الأخير فإن ما يمكن قوله بهذا الخصوص أن المديرية العامة للأمن الوطني تولي أهمية بالغة في مجال مكافحة الإجرام المعلوماتي ، غير انها و بالنظر إلى الدول الأجنبية الأخرى لا تزال متأخرة

---

[1] – ملخص الزيارة الميدانية لدائرة الأدلة الرقمية و الآثار التكنولوجية – المخبر الجهوي للشرطة العلمية لولاية قسنطينة بتاريخ : 01 أفريل 2015.

[2] – ملخص الزيارة الميدانية لدائرة الأدلة الرقمية و الآثار التكنولوجية – المخبر الجهوي للشرطة العلمية لولاية قسنطينة بتاريخ : 01 أفريل 2015.

بعض الشيء من حيث قلة عدد و عتاد هذه الوحدات هذا من جهة، إضافة إلى العقبات التشريعية التي تحد من عمل أعضاء هذه الوحدات كشرط الحصول على تسخيرة من قبل الجهات القضائية المختصة لأجل الإنطلاق في أعمال البحث و التحقيق المعلوماتي و لو وصل إلى علم أعضائها تبليغات من قبل الضحايا أنفسهم ، أو معلومات بوقوع جريمة معلوماتية ، و هو ما يضيق من مجال عملهم و يحد من مدى فعاليتهم في دعم أعمال البحث و التحقيق، نظرا لطول مدة إستيفاء الإجراءات القانونية و ما يصاحبها من فقدان للأدلة الإلكترونية ، نظرا لقدرة الجاني على التخلص من أثارها و محوها قبل وصول أيدي هؤلاء إليها ، و هو ما يدعونا إلى لفت إنتباه القائمين على شؤون مؤسسة الأمن الوطني إلى ضرورة وضع نصوص ملائمة بالتنسيق مع الجهات القضائية تمنح حرية اكبر في مسائل مباشرة الإجراءات الخاصة بالمتابعة و التحقيق في الجرائم المعلوماتية ، نظرا لسرعة تنفيذ و محو أدلة هذه الأخيرة.

الفرع الثالث: الوحدات التابعة للدرك الوطني الجزائري.

يضع الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن و النظام العام و محاربة الجريمة بكافة انواعها، وحدات متنوعة و عديدة على مستوى القيادة العامة ، او على مستوى القيادات الجهوية و المحلية و هي تباعا :

1. قيادة الدرك الوطنية.
2. الوحدات الإقليمية.
3. الوحدات المشكّلة.
4. الوحدات المتخصّصة وحدات الإسناد.
5. هياكل التكوين.
6. المعهد الوطني للأدلّة الجنائية وعلم الإجرام.

7. المصالح والمراكز العلمية والتقنية.

8. المصلحة المركزية للتحريات الجنائية .

9. المفرزة الخاصّة للتدخل[1].

تعمل مؤسسة الدرك الوطني جادة إلى التطلع بمختلف الجرائم المرتكبة على شبكة الإنترنت و هذا لتسهيل مهمة البحث و المعاينة و التفتيش في أنظمة الحواسيب و العمل على مراقبة مختلف الشبكات، و بالتالي فقد تم وضع مصالح الشرطة القضائية التابعة للدرك الوطني في خدمة هذه الأهداف، و ذلك حسب الإختصاص و الصلاحيات و طبيعة الجريمة إلى ثلاث 03 مستويات مركزية، جهوية ، محلية.

الفقرة الأولى : على المستوى المركزي .

تعمل مصالح الدرك الوطني من خلال أجهزتها المركزية على مكافحة الجرائم المعلوماتية و دعم اعمال البحث و التحقيق بشأنها من خلال الهيئات التالية :

أولا – مديرية الأمن العمومي و الإستغلال : و هي الهيئة التي تعمل على التنسيق بين مختلف الوحدات الإقليمية و المركز التقني العلمي، في مجال أعمال البحث و التحري في الجرائم المعلوماتية.

ثانيا – المصلحة المركزية للتحريات الجنائية : و هي هيئة ذات إختصاص وطني من بين مهامها مكافحة الجريمة المرتبطة بتكنولوجيا الإعلام و الإتصال[2] .

---

[1] – الموقع الرسمي لقيادة الدرك الوطني – تاريخ التصفح 31 مارس 2015 – الرابط الإلكتروني :
http://www.mdn.dz/site_cgn/index.php?L=ar&P=undefined

[2] – معلومات مقدمة من قبل الفرقة الإقليمية للدرك الوطني – بسكرة– الجزائر.

ثالثا – المعهد الوطني للأدلة الجنائية و علم الإجرام : يعد المعهد الوطني للأدلة الجنائية وعلم الإجرام مؤسسة عمومية ذات طابع إداري، تم إنشاءه بمرسوم رئاسي رقم 183-04 بتاريخ : 26 جوان 2004، في إطار عصرنة قطاع الدرك الوطني، وهو يشكل كذلك أداة مستلهمة من الخبرات التطبيقية و التحاليل الحديثة والمدعومة بالتكنولوجيات المناسبة، يعد المعهد بمثابة هيئة مختصة في إجراء الخبرات و المعاينة و ذلك بمختلف دوائره ، بما فيها **دائرة الإعلام الآلي و الإلكترونيك** ،التي أوكلت لها مهام تحليل الأدلة الخاصة بالجرائم المعلوماتية ، و ذلك بتحليل الدعامات الإلكترونية ، و إصلاح الدعامات التالفة ، إنجاز المقاربات الهاتفية ، تحسين التسجيلات الصوتية و الفيديو و الصورة و ذلك لتسهيل إستغلالها .

إن الخدمة الاساسية التي يقدمها هذا المعهد هي خدمة العدالة ودعم وحدات التحري في إطار مهام الشرطة القضائية ، ولهذا فإن المعهد الوطني للأدلة الجنائية وعلم الإجرام يساهم بشكل فعال في مكافحة الجرائم المعلوماتية من خلال مهامه الخاصة بمتابعة أو دعم إجراءات البحث و التحقيق في الجرائم المعلوماتية فهو يتولى في هذا الشأن :

- القيام بالخبرات العملية أو الخبرات اللازمة في توجيه التحقيقات القضائية بطلب من القضاة من أجل كشف الحقيقة بالأدلة العلمية لتحديد هوية مرتكبي الجنايات و الجنح، بما فيها تلك المتعلقة بالجرائم المعلوماتية.
- مساعدة المحققين للسير الحسن للمعاينات، عن طريق دعمهم الأفراد المؤهلين أثناء الحاجة.
- تنفيذ مناهج الشرطة العلمية و التقنية لجمع وتحليل الأدلة المأخوذة من مسرح الجريمة.
- ضمان المساعدة العلمية في التحريات المعقدة كحال التحريات الخاصة بالجرائم المعلوماتية.
- المشاركة في الأبحاث والتحاليل المتعلقة بالوقاية للتقليل من جميع أشكال الإجرام بما فيها المعلوماتي.

- مشاركة و مساهمة المعهد الوطني للأدلة الجنائية وعلم الإجرام بصفته الهيئة المكلفة بالتحاليل والخبرات في ميدان علم الإجرام في وضع سياسة مكافحة الإجرام[1].

رابعا – مركز الوقاية من جرائم الإعلام الآلي و الجرائم المعلوماتية : أنشأ هذا المركز حديثا و يعتبر بمثابة نقطة وصل وطنية في مجال دعم اعمال البحث و التحقيق في الجرائم المعلوماتية [2]، إذ يوفر المساعدة التقنية للمحققين و يساهم في توجيه التحقيقات المرتبطة بتكنولوجيا الإعلام و الإتصال ، فهو هيئة تقنية تعمل تحت وصاية مديرية الأمن العمومي و الإستعمال لقيادة الدرك الوطني و يحقق المهام التالية :

1. ضمان المراقبة الدائمة و المستمرة على شبكة الإنترنت.
2. القيام بمراقبة الإتصالات الإلكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني و الجهات القضائية.
3. مساعدة الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المرتبطة بتكنولوجيا الإعلام والإتصال و البحث عن الأدلة في شبكة الأنترنت.
4. المشاركة في عمليات التحري و التسرب عبر شبكة الأنترنت لفائدة وحدات الدرك الوطني و السلطات القضائية .
5. المشاركة في قمع الجرائم المعلوماتية، من خلال التعاون مع مختلف مصالح الأمن و الهيئات الوطنية.[3]

---

[1] – الموقع الرسمي لقيادة الدرك الوطني – تاريخ التصفح 31 مارس 2015 – الرابط الإلكتروني :
http://www.mdn.dz/site_cgn/index.php?L=ar&P=undefined

[2] – عالج هذا المركز في الـ 10 أشهر الأولى من سنة 2015 ما يقارب 240 قضية متعلقة بالجرائم المعلوماتية ، تونعت بين جرائم التهديد، المساس بالنظام العام، جرائم الإختراق، التحرش الجنسي بالقصر و تحريضهم على الفيق و الدعارة، إهانة هيئات و رموز وطنية ، النصب و الإحتيال، الإعتداء على حرمة الحياة الخاصة . أنظر في ذلك : عزالدين عزالدين – قيادة الدرك الوطني– الإطار القانوني للوقاية من الجرائم المعلوماتية و مكافحتها – بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة– 16و 17 نوفمبر 2015– كلية الحقوق – جامعة بسكرة– الجزائر ص29.

[3] – معلومات مقدمة من قبل الفرقة الإقليمية للدرك الوطني – بسكرة– الجزائر.

إذن تعتبر هذه الهيئات التابعة للدرك الوطني مسؤولة عن تنفيذ إجراءات البحث و التحقيق بشأن الجرائم المعلوماتية ، و ذلك على نطاق وطني بحيث تعتبر هيئات دعم و إسناد و نقاط و صل بين مختلف الوحدات الأخرى المتخصصة و التي توجد كذلك على مستويات أدنى منها الجهوية و المحلية .

الفقرة الثانية : على المستوى الجهوي .

تختص المصالح الجهوية للشرطة القضائية التابعة للدرك الوطني بمهمة تنسيق النشاطات بين مختلف الوحدات التابعة للشرطة القضائية و كذلك دعمها بالوسائل الخاصة للتحريات و الأبحاث المعقدة كالجرائم المعلوماتية.

يلعب الدرك الوطني دورا هاما في ميدان الشرطة القضائية نظرا لانتشار وحداته على مستوى كامل التراب الوطني، ونظرا للوسائل المادية الموضوعة تحت تصرفه وعدد أفراده الهائل، والصلاحيات التي خولها لهم القانون ، و هم في الواقع حسب الرتب والوظائف ضباط وأعوان الشرطة القضائية.

الفقرة الثالثة : على المستوى المحلي .

يحوز الدرك الوطني على فصائل للأبحاث التي ينتمي إليها أفراد ذوو خبرة وإختصاص واسعين في ميدان الشرطة القضائية، هذه الفصائل مكلفة خصوصا بمكافحة الأشكال الخطيرة للإجرام المنظم كالجرائم المعلوماتية ، وذالك عن طريق القيام بتحقيقات تتطلب تحريات معقدة ، هذه الوحدات المختصة تساهم في تدعيم نشاط الأبحاث والتحريات التي تقوم بها الفرق الإقليمية للدرك الوطني.

هذه الأخيرة أعيد تنظيمها بتاريخ 21 جويلية 2007 بموجب التعليمة رقم 4-223-2007 الصادرة عن ديوان قيادة الدرك الوطني ، و ذلك للتماشى مع طبيعة الجرائم محل المعاينة ، و هو ما سمح بإنشاء

خلية متخصصة لمكافحة الجرائم المتعلقة بتكنولوجيا الإعلام و الإتصال في سبعة عشرا 17 مجموعة ولائية ، و هو ما يسمح بتطبيق سياسة فعالة في مكافحة الجرائم المعلوماتية من خلال توفير اخلايا المتخصصة في مجال أعمال البحث و التحقيق في هذا النوع من الجرائم .[1]

إن كل المعطيات التي إستعرضناها في هذا المبحث توضح و بشكل جلي مدى تكاثف و تعزيز الجهود المتعلقة بترقية و دعم أعمال البحث و التحقيق بشأن الجرائم المعلوماتية ، من خلال تصنيفها على حدى و تخصيص أجهزة أمنية خاصة بمباشرة الأعمال المتعلقة بالبحث و التحقيق بشأنها ، و ذلك نظرا لخصوصيتها من جهة و لخصوصية مرتكبيها و أدلتها من جهة أخرى ، غير ان الملاحظ بشأن ذلك هو مدى التفاوت الحاصل بين الجهود المبذولة و النتائج المحصلة في هذا المجال ، فعلى المستوى الإقليمي الأروبي فإننا نلاحظ مدى الإهتمام بترقية و دعم مجال اعمال البحث و التحقيق في الجرائم المعلوماتية من خلال حجم الوحدات ذات الإختصاص الدولي و الإقليمي و الداخلي ، التي أصبحت تعمل على مكافحة هذا النوع من الجرائم ، عكس ذلك هناك شبه غياب للتعاون على المستوى الإفريقي و العربي بهذا الخصوص ، و ذلك راجع أساسا إلى ضعف الإمكانيات المادية و البشرية في هذا المجال بالرغم من الإنتشار الفائق لتقنية المعلوماتية ، و هو ما ينعكس على معدلات تنامي الإجرام المعلوماتي في هذه الدول و إزدياد عدد حالاتها .

[1] – معلومات مقدمة من قبل الفرقة الإقليمية للدرك الوطني – بسكرة– الجزائر.

خلاصة الفصل.

إن المعطيات المستعرضة في هذا الفصل تسمح لنا بالقول بإن الإهتمام التشريعي و القانوني بالظاهرة الإجرامية المعلوماتية سواء من الناحية الموضوعية او الإجرائية خصوصا ، لم يكن سوى وليد الجدل الفقهي الذي سبق و أن قام بين مؤيد و معارض لطبيعة للجريمة المعلوماتية ، بين معنوية لا مكانة لها بين فصول القوانين العقابية ، و بين آخر قائل بأنها ذات طبيعة خاصة و بأنه يجب إستحداث مركز قانوني خاص بها ، و هو الرأي الذي تم تبني أفكاره نظرا لما شهدته هذه الجرائم من إرتفاع في معدلاتها و درجة خطورتها ، و حجم أثارها و نتائجها التي أصبحت و في ظل كل ذلك تشكل تهديدا حقيقيا على الأمن العام و الخاص ، و هو ما إستدعى و على عجلة إستحداث نصوص قانونية خاصة تنظم عمل و سير إجراءات البحث و التحقيق في مجال الجرائم المعلوماتية بالرغم من طابعها المعنوي ، و ذلك تحت ضغط الظاهرة الإجرامية و فرضها لمجموعة من المتغيرات و التحديات القانونية و الفنية و الإجرائية الحديثة التي لم تكن متصورة من قبل ، و قد تترجم الإهتمام التشريعي في مجوعة من النصوص على المستوى الدولي في شكل إتفاقية بودابست لمكافحة الجرائم المعلوماتية لسنة 2001 ، و كذلك الإتفاقية العربية لمكافحة الجرائم المتصلة بتكنولوجيا المعلومات لسنة 2010 ، و هي الإتفاقيات التي شكلت نماذج عمل للتشريعات الداخلية لما تحمله من مبادئ أساسية في تجريم السلوكات المعلوماتية غير المشروعة ، أو في مجال و ضع الأسس الإجرائية في مجال أعمال البحث و التحري في الجرائم المعلوماتية ، و هو ما إقتدى به المشرع الجزائري سنة 2009 من خلال سنه لقانون مكافحة الجرائم المتصلة بتكنولوجيات الإعلام الإتصال تحت رقم 09-04 ، و الذي حاول من خلاله المشرع وضع أسس قانونية تنظم مجال الإجراءات الخاصة بعمليات البحث و التحري في الجرائم المعلوماتية خصوصا و ان قانون الإجراءات الجزائية الجزائري مازال يخلو من هذا الجانب الإجرائي الخاص، و هي الإرادة التي جسدها صدور المرسوم

الرئاسي رقم 15-261 الصادر بتاريخ 08 أكتوبر 2015 الذي تم بموجبه إنشاء الهيئة الوطنية المكلفة بالوقاية و بمكافحة الجرائم المعلوماتية ، و تحديد كيفيات سيرها و عملها.

و كنتيجة لكل ما سبق ذكره يمكننا تلخيص مجموعة النتائج المتوصل إليها حسب التالي:

- تكييف الفقه و القانون مع الجريمة المعلوماتية ، و ذلك من خلال الإعتراف لها بالمركز القانوني المستقل ، و العمل على إيجاد الحلول الفعالة في مجال دعم أعمال البحث و التحقيق ، و تفادي الإشكاليات التي تطرحها هذه الإجراءات في مواجهة النصوص القانونية الإجرائية ، التي تعترف في غالبية نصوصها بشرعية الإجراءات المتخذة في مواجهة الجرائم المادية التقليدية ، مع ضعف بارز في التعامل مع الجانب الإجرائي في مواجهة الجرائم المعلوماتية ، و هو ما يولد ثغرات قانونية تظهر أثارها أثناء مباشرة الإجراءات، فينتج عنها إما هدر للحق العام من خلال إتاحة الفرصة للمتهم للفرار من قبضة العدالة ، او هدر للحريات الفردية من خلال التعسف في تفسير النصوص .
- تكاثف الجهود التشريعية في العشرية الأخيرة على كافة المستويات الدولية منها خصوصا و الإقليمية و الداخلية، في سبيل و ضع حلول نهائية لإشكالية تعارض نطاق العالمية الذي يميز الجريمة المعلوماتية ، و مبدأ إقليمية النص الجنائي ، و المبادئ الإجرائي المتعلقة بالإختصاص الإقليمي التي تحكم عمل الجهات المخول لها مباشرة إجراءات البحث و التحقيق، و التي تعتبر عائقا حقيقيا في مسار نجاح إجراءات البحث و التحقيق في الجرائم المعلوماتية ، نظرا لإرتباطها بمفهوم السيادة و عدم تكافؤ الإمكانيات في مجال تفعيل تعاون دولي فعال .
- تبني سياسة أمنية تعتمد على مبدأ التخصص في ميدان مكافحة الجريمة المعلوماتية ، من خلال إستفراد وحدات خاصة بمسائل البحث و التحقيق في الجرائم المعلوماتية ، و ذلك على المستوى الدولي و الإقليمي ، و كذلك الداخلي ، و هو ما حاولنا إبرازه من خلال ما إستعرضناه تبعا في المبحث الثاني

من فصلنا هذا ، و هي السياسة التي أثبتت نجاعتها في هذا المجال بدليل نجاح هذه الوحدات و الفرق الخاصة بالإطاحة بأكبر الشبكات في مجال الإجرام السيبرني ، و القبض على مرتكبيها و تقديمهم امام العدالة ، في ظل عدم كفاءة و قدرة الوحدات الأخرى على تحقيق نفس الأهداف بسبب عدم تخصصها بمجال المعلوماتية ، و هي النتائج التي أضحت تتحقق دوريا من خلال جهود الوحدات الخاصة التابعة للهيئة الوطنية للوقاية و مكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال، و كذلك الخلايا الأمنية التابعة للمديرية العامة الوطنية للأمن الوطني و المختصة بمكافحة الجرائم المعلوماتية و التي تنتشر عبر كافة التراب الوطني ، شأنها شأن تلك الوحدات المتخصصة التابعة للقيادة العامة للدرك الوطني الجزائري ، في ظل سياسة مكافحة الجرائم المعلوماتية المتبناة من قبل المشرع الجزائري أملا منه في وضع حد للظاهرة الإجرامية المعلوماتية خصوصا في ظل تفتح المجتمع الجزائري على التقنية المعلوماتية في الآونة الأخيرة .

و بناء على ما سبق جاز لنا التساؤل عن مدى فعالية الحلول التشريعية و العملية ، في ميدان مكافحة الجرائم المعلوماتية ، و ذلك من خلال أساليب عملها و الوسائل التي تعتمدها و الأهداف و النتائج التي تتوخاها أثناء مباشرة أعمال البحث و التحقيق في الجرائم المعلوماتية ؟ و هو ما سنستعرضه في الفصل الموالي لبحثنا هذا .

الفصل الثالث

الإجراءات الخاصة بالبحث و التحقيق في الجرائم المعلوماتية و أثارها

مما لاشك فيه أنه لا يوجد ما يسمى بالجريمة الكاملة مهما حاول الجاني إخفائها، و ذلك استنادا لقاعدة " **لوكارد** "[1] لتبادل المواد التي تنص على أنه عند احتكاك جسمين ببعضهما البعض فإنه لابد أن ينتقل جزء من الجسم الأول إلى الثاني وبالعكس ، و بالتالي ينتج عن هذا الاحتكاك الدليل الجنائي ، و في مجال الجريمة المعلوماتية ينتج لدينا ما يعرف بالدليل الالكتروني أو ما يطلق عليه بالدليل الرقمي[2].

ونظرا لطبيعة الجرائم المعلوماتية الخاصة فإنها تتطلب إجراءات و أساليب خاصة و نوعية للبحث و التحقيق، لأجل اكتشاف الدليل الرقمي و تحصيله من قبل الفنيين المختصين، و كل ذلك يستدعي اتخاذ إجراءات سريعة[3].

إن إجراءات البحث التحقيقي الجنائي العام هي الأساس في البحث و التحقيق في جرائم المعلوماتية تماما كما هو الحال في باقي الجرائم الأخرى، أما عناصر البحث و التحقيق الجنائي الأخرى من معملية و فنية و غيرها فإن استخدامها يتوقف على ظروف كل جريمة ، فالملاحظ أن إجراءات التحقيق في

---

[1] – Le principe d’échange de Locard, énoncé pour la première fois par Edmond Locard en 1920 s’applique au lieu du crime, à l’auteur, à la victime, il peut s’exprimer de la manière suivante :
–l’auteur et/ou son matériel abandonnent des indices sur la victime et sur la scène de crime.
L’auteur et /ou son matériel emportent des indices appartenant a la victime et a la scène de crime. Plus d’information voir :
–Jean Claude martin – investigation de scènes de crimes –fixation de l’état des lieux et traitement des traces d’objet– presse polytechnique et universitaire Romandes– France– 2004. P 08.

[2] – عائشة بن قارة– مرجع سابق– ص 78.

[3] – عبد الله سعود بن محمد السراني– مرجع سابق –ص 65.

الجرائم المعلوماتية تتصف بالخصوصية من حيث طريقة كشفها و التبليغ عنها، و العناية بمسرح الجريمة و كيفية تكوين فريق الضبط و التفتيش، وصولا إلى خصوصية التعامل مع الأدلة الجنائية[1].

إذن كل هذه الإجراءات ذات الطابع الإجرائي يجب أن تتم بالموازاة مع طبيعة الجريمة المعلوماتية و ما ينتج عنها من خصوصيات تغيب عن الجرائم الأخرى، و هو ما يتجلى في خصوصيات عمل رجال البحث و التحقيق المنوط بهم مهام البحث و التحقيق المعلوماتي، و هو ما يدفعنا إلى طرح التساؤل حول طبيعتها الإجرائية العملية في مجال البحث و التحقيق المعلوماتي؟ و إلى أي مدى تظهر نجاعة هؤلاء في حل طلاسم الجرائم المعلوماتية بالرغم من تعقيدها و تشعبها؟ و هل الدليل الجنائي يعتبر دليلا على قدم المساواة من حيث قوته الثبوتية و باقي وسائل الإثبات الأخرى؟ إن الإجابة عن هذه الإشكالية الفرعية تستدعي هنا تقسيم هذا الفصل إلى مبحثين أساسيين هما:

- **الأول:** نستهله لمعالجة خصوصيات عمل رجال البحث و التحقيق المعلوماتي و الأساليب المتبعة من قبلهم في هذا الشأن.
- **الثاني:** فسنخصصه لمعالجة مسألة الدليل الإلكتروني الناتج عن عمل رجال البحث و التحقيق المعلوماتي و مدى حجيته في مجال الإثبات الجنائي.

---

[1] - ضياء علي أحمد النعمان- الغش المعلوماتي الظاهرة والتطبيقات- الطبعة الأولى- المطبعة الوطنية- المملكة المغربية- 2011 - ص 363.

المبحث الأول: الإجراءات الخاصة المتبعة في إطار تنفيذ إجراءات البحث و التحقيق المعلوماتي.

كما سبق و أن فصلنا بشأن الجريمة المعلوماتية، التي تعتبر و من حيث طبيعتها جريمة فريدة من نوعها، و كذلك الشأن من حيث محلها، أثارها، أشخاصها، فهي جريمة ناعمة لا تعتمد على العنف المادي أو صور التعدي على الغير المادية، فهي تستهدف النظم المعلوماتية بما تحتويه من معطيات و بيانات و معلومات و التي تعتبر في نظر المجرم المعلوماتي أكبر قيمة مما قد يتصوره المجرم التقليدي، و هي بنتائجها أشد خطورة من بعض الجرائم التقليدية بالرغم من خلوها من مظاهر العنف المادي فنتائجها تتسبب في تعطل المصالح العليا للدول، و لأكبر الشركات، و كذلك بالنسبة للأفراد نظرا لما قد تسببه لهم من ضرر مادي و معنوي سواء مست بذمتهم المالية أو بحقوقهم الشخصية و المعنوية.

و نظرا لاهتمام الجانب القانوني بمسائل تجريم هذا النوع من السلوكات فإنه وضع في سبيل ذلك شقا إجرائيا خاصا، يهدف إلى مكافحة هذه الجريمة من خلال تتبع مرتكبيها من أجل توقيع العقاب بحقهم،[1] هذا الشق الإجرائي المتضمن ضمن قواعد قانون الإجراءات الجزائية و بعض النصوص الإجرائية ذات الطبيعة الخاصة، يحمل في فحواه بعض الخصوصيات و الشروط الواجب اتباعها لأجل إضفاء طابع الشرعية الإجرائية على أعمال جهات البحث و التحقيق ، و لأجل تحقيق فعاليتها القصوى في سبيل تحصيل الدليل الالكتروني، الذي يمكنهم من معرفة هوية الفاعل و تقديمه أمام الجهات

---

[1] –تم تسجيل سنة 2012 على مستوى المحاكم الجزائية الفرنسية **2222 حالة إدانة** في قضايا مصنفة في خانة الجرائم المعلوماتية ، موزعة بين الجنايات و الجنح تصدرتها الجرائم الماسة بالأشخاص بـ 817 إدانة ، تليها جرائم المساس بالنظام العام بـ 800 حالة ، لتأتي جرائم الإستعمال غير المشروع لأدوات الدفع الإلكتروني بـ 321 حالة ، و كذلك جرائم المساس بالأنظمة المعلوماتية بـ 182 حالة ، لتتوزع باقي الحالات على جرائم اخرى . أنظر في ذلك: تقرير مجموعة العمل الحكومية المشتركة الفرنسية 2014– مرجع سابق– ص28.

القضائية لمواجهته بالأدلة المتحصلة من عمليات البحث و التحقيق بشأن جريمته،و هي المسائل التي نستعرضها في هذا المبحث الذي نتعرض من خلاله إلى معالجة ثلاث مطالب رئيسية نعالج فيها الواحد تلو الأخرى خصوصيات آليات عمل هيئات البحث و التحقيق المعلوماتي بدءا بتحديد الشروط القانونية و الفنية التي يجب أن تتوفر في شخص المحقق (المطلب الأول).

ثم مسألة المهارات الفنية الواجب توفرها لدى رجال البحث و التحقيق المعلوماتي، و التي تسمح لهم تأدية مهامهم بالأسلوب المناسب مع الجريمة المعلوماتية (المطلب الثاني).

و أخيرا نعالج مسائل الإجراءات الخاصة بمرحلة الانتقال إلى مسرح الجريمة المعلوماتية لأجل مباشرة أعمال المعاينة و الضبط (المطلب الثالث).

المطلب الأول: الشروط الخاصة بالمحقق في جرائم المعلوماتية.

لا تجيز الجريمة المعلوماتية و بحكم خصوصيتها و طبيعتها، لأي كان من جهات الضبطية القضائية أو جهات التحقيق أو النيابة العامة أمر البحث و التحقيق بشأنها، فهي جريمة تستلزم محققا من نوع خاص قادر على التعامل مع مميزاتها بالشكل اللازم الذي يسمح له بمعرفة هوية مرتكبها و تحديد معالمها و آثارها، و ذلك من خلال تتبع آثارها الالكترونية و دلائلها، كل ذلك في إطار الشرعية الإجرائية ، تجنبا لطائلة البطلان و احتراما لحقوق و حريات الأفراد.

إن الإجراءات الخاصة بالبحث والتحقيق في مجال الجرائم المعلوماتية، المحددة وفق القواعد العامة لقانون الإجراءات الجزائية أو بعض القوانين الأخرى المكملة له على شاكلة القانون 09 – 04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و سبل مكافحتها، سواء تلك المتعلقة بالاختصاص النوعي و الإقليمي، تعتبر في مجملها قاصرة في مجال تحديد الصفات الملائمة لرجال البحث و التحقيق في الجرائم المعلوماتية و ذلك بسبب وجوب توفر

شروط أخرى خاصة في شخص المحقق ذاته حتى يكون على استعداد لمواجهة تحديات الجرائم المعلوماتية، و هي الشروط المتعلقة بالمعرفة الفنية للنظم المعلوماتية ، و التي تعتبر مكملا أساسيا لجملة الشروط القانونية التقليدية، و هو ما سنستعرضه في الفرعين المواليين اللذان خصصنا أولهما لتحديد الشروط القانونية المشترطة في شخص المحقق المعلوماتي، و ثانيهما لجملة الشروط المعرفية و الفنية بالنظم المعلوماتية التي يجب أن يحيط بها المحقق حتى يحسن التعامل مع الجريمة المعلوماتية.

الفرع الأول: الشروط المتعلقة بالاختصاص القضائي.

تعتبر شروط الاختصاص القضائي من مسائل النظام العام التي يمكن إثارتها في أي مرحلة كانت عليها الدعوى فتتعرض الإجراءات برمتها للبطلان في حال عدم استيفائها، و شروط الاختصاص في مسائل البحث و التحقيق نوعان اختصاص نوعي و آخر إقليمي محلي، فلا يمكن لمن يتولى أعمال البحث و التحقيق مباشرة أعماله و هو غير مختص نوعا ، كما لا يمكن لمن يتولى الإجراءات نفسها و هو يتمتع بصفة الاختصاص النوعي ممارسة أعماله خارج نطاق اختصاصه الإقليمي.

الفقرة الأولى: تحديد مفهوم شروط الاختصاص النوعي في مسائل الجريمة المعلوماتية.

تعتبر إجراءات البحث و التحقيق من الإجراءات التي تمس بحقوق و حريات الأفراد، و لذلك فقد حرص المشرع الجزائري على اسنادها لجهة قضائية لأجل ضمان كفالة حقيقية لجملة الحقوق و الحريات الفردية، و تتمثل عادة هذه الجهة القضائية في هيئة الضبطية القضائية إذا كانت الإجراءات متعلقة بمرحلة البحث و التحري ، و في هيئة قضاء التحقيق إذا كانت الإجراءات متعلقة بمرحلة التحقيق القضائي ممثلة في شخص قاضي التحقيق .[1]

---

[1] – تعمل كل من الضبطية القضائية على القيام بأعمال البحث و التحري عن الجرائم ما لم يبدأ فيها بتحقيق قضائي و ذلك من قبل ضباط و أعوان الشرطة القضائية و كذلك بعض الأعوان المنوط بهم مثل هذه المهام و ذلك تحت إدارة وكيل الجمهورية و إشراف النائب العام للمجلس القضائي التابعين له ، و تحت رقابة غرفة

و كما سبق و أن وضحنا سابقا فإن الاختصاص العملي و الفني في مجال أعمال البحث و التحقيق في الجرائم المعلوماتية يعود و بالدرجة الأولى إلى دائرة مكافحة الجرائم المعلوماتية التابعة للمديرية العامة للأمن الوطني، و كذلك الفرق التابعة لمركز الوقاية من جرائم الإعلام الآلي و الجرائم المعلوماتية و مكافحتها التابعة لسلك الدرك الوطني ، و إلى مديرية المراقبة الوقائية و اليقظة الإلكترونية التابعة للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها و تحت إشرافها، و التي تم الإعلان عن إنشائها رسميا بموجب صدور المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015 ، هذه الوحدات الخاصة تتكون أساسا من جملة من المستخدمين يتولى ممن تتوفر لديهم صفة ضباط للشرطة القضائية مباشرة إجراءات البحث و التحقيق في الجرائم المعلوماتية، إما من تلقاء أنفسهم أو بناء على طلبات و اوامر تردهم من قبل وكيل الجمهورية أو قاضي التحقيق ، مما يجعل منهم العنصر البارز في متابعة هذه الإجراءات بصفة فعلية دون غيرهم.

الفقرة الثانية: اختصاص ضباط الشرطة القضائية بالبحث و التحري في مجال الجرائم المعلوماتية.

يتولى عادة ضباط الشرطة القضائية مسائل البحث و التحري في كافة الجرائم ، بما في ذلك الجرائم المعلوماتية فلا يوجد مانع قانوني يحد من ممارسة هؤلاء لأعمالهم المتعلقة بالبحث و التحري في مجال الجرائم المعلوماتية بعد تبليغهم بوقوعها[1]، سوى أن يتوفر فيهم شرط الاختصاص النوعي و الذي يمكن تحديده في التمتع بصفة ظابط الشرطة القضائية، و ذلك تقيدا بما يفرضه نص المادة 05 من الفصل الثالث المتعلق بالقواعد الإجرائية الخاصة بتفتيش النظم المعلوماتية الوارد في نص القانون

الإتهام ، و إذا ما أفتتح تحقيق قضائي بشأن تلك الجرائم تحول دورهم إلى تنفيذ تفويضات جهة التحقيق و تنفيذ طلباتها- راجع نصوص المواد 12 إلى 14 من قانون الإجراءات الجزائية الجزائري.

[1] - المادة 17 - الفقرة 01 قانون الإجراءات الجزائية الجزائري المعدل بموجب الأمر رقم 15-02 المؤرخ في 23 جويلية 2015.

09 – 04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و سبل مكافحتها و التي تنص على أنه: " يجوز للسلطات القضائية المختصة و كذا ضابط الشرطة القضائية في إطار قانون الإجراءات الجزائية ... الدخول بغرض التفتيش و لو عن بعد إلى منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتية المخزنة فيها ... ".

و بناء على ذلك فأن الأشخاص المذكورين في نص (المادة 15 ق 2/85) من قانون الإجراءات الجزائية الجزائري، و التي تحدد قائمة حصرية لصفة الأشخاص المنوط بهم هذه الصفة، هم الأشخاص المخولون قانونا بمباشرة أعمال البحث و تنفيذ أوامر التحقيق بشأن الجرائم المعلوماتية .[1]

إن المتمعن في نص المادة و حسب رأينا الخاص، لا يتصور أن يقوم رئيس المجلس الشعبي البلدي بتولي أعمال البحث و التحقيق في الجرائم المعلوماتية ، فحسب ما بيناه سالفا فإن هذا الإختصاص يعود و بالدرجة الأولى لضباط الشرطة القضائية المنتمين إلى الفرق المتخصصة في مكافحة الجرائم المعلوماتية ، و التي تضم محققين من نوع خاص كما سنبينه لاحقا ، و لذلك وجب تخصيص نص منفرد

---

[1]– جاء في نص المادة 15 من قانون الإجراءات الجزائية الجزائري المعدلة بموجب الأمر 15–02 المؤرخ في 23 جويلية 2015 انه :" يتمتع بصفة ضابط الشرطة القضائية :

- رؤساء المجالس الشعبية البلدية.
- ضباط الدرك الوطني.
- الموظفون التابعون للأسلاك الخاصة للمراقبين و محافظي و ضباط الشرطة للأمن الوطني.
- ذوو الرتب في الدرك، و رجال الدرك الذين أمضوا في سلك الدرك ثلاث سنوات غلى الأقل و الذين تم تعينهم بموجب قرار مشترك بين وزير العدل ووزير الدفاع الوطني ، بعد موافقة لجنة خاصة.
- الموظفون التابعون للأسلاك الخاصة للمفتشين و حفاظ و اعوان الشرطة للأمن الوطني الذين أمضوا ثلاث 03 سنوات على الأقل و عينوا بموجب قرار مشترك صادر عن وزير العدل ووزير الداخلية و الجماعات المحلية بعد موافقة لجنة خاصة.
- ضباط و ضباط الصف التابعين للمصالح العسكرية للأمن الذين تم تعيينهم خصيصا بموجب قرار مشترك صادر بين وزير الدفاع و وزير العدل".

في قانون الإجراءات الجزائية يحدد الإختصاص النوعي في شخص رجال الشرطة و الدرك و الأمن العسكري الموظفون التابعون للأسلاك الخاصة للمراقبين ،ممن يتمتعون بصفة ضباط الشرطة القضائية ، حتى يتحقق الإنسجام بين النص العام و النص الخاص ممثلا في القانون 09-04 ، و ذلك تجنبا لتداخل الإختصاصات و تضيع فرص إحراز الأدلة ، و التسبب في إفلات الجاني من المتابعة والعقاب.

إذن فمن أجل حق ممارسة أعمال البحث و التحري(التحقيق الإبتدائي) في الجرائم المعلوماتية، فإن الشرط الأساسي هو التمتع بصفة ضابط الشرطة القضائية و ذلك حسب ما هو وارد في هذا الشأن بموجب نص (المادة 63 ق 06-22) قانون الإجراءات الجزائية الجزائري بقولها :" يقوم ضباط الشرطة القضائية ، و تحت رقابتهم أعوان الشرطة القضائية ، بالتحقيقات الإبتدائية بمجرد علمهم بوقوع الجريمة إما بناء على تعليمات وكيل الجمهورية او من تلقاء انفسهم " .

كما يجوز لضباط الشرطة القضائية القيام بكل أعمال التحقيق القضائي اللازمة لكشف الحقيقة في مجال الجرائم المعلوماتية ، إذا ما تعذر على قاضي التحقيق القيام بها بنفسه ، و ذلك بعد نبدهم من قبل هذا الأخير حسب الشروط القانونية المنصوص عليها في المواد من 138 إلـى 142 من قانون الإجراءات الجزائية ، و على قاضي التحقيق عند إنتهاء هؤلاء من أعمالهم مراجعة عناصر التحقيق.[1]

و لقد أجاز المشرع حسب مضمون الفقرة الأخيرة من (المادة 05 ق 04 – 09) المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و سبل مكافحتها ، و في سبيل تخطي عقبات انعدام المعرفة الفنية بالنظم المعلوماتية من قبل ضابط الشرطة القضائية ، لهؤلاء أن يقوموا بتسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث بقصد مساعدتهم و تزويدهم بكل المعلومات الضرورية

---

[1]– الفقرة 06 و 07 – المادة 68 ق 01-08 قانون الإجراءات الجزائية الجزائري.

لإنجاز مهامهم دون أن تتعرض الإجراءات المتخذة للبطلان ، و هو ما أكدته المادة 65 مكرر 8 ق 06 – 22 قانون الإجراءات الجزائية الجزائري ، و هي نفس القواعد التي حددها المشرع الفرنسي بموجب نصوص المواد 227 – 18 إلى 227 – 24 قانون العقوبات الفرنسي.

الفقرة الثالثة: الإختصاص النوعي للجهات القضائية (النيابة العامة – قضاء التحقيق).

أولا: جهة النيابة العامة: تعتبر النيابة العامة السلطة المختصة بمباشرة الدعوى العمومية باسم المجتمع و تتولى مهمة المطالبة بتطبيق القانون[1] ، و يتولى النائب العام مهمة تمثيل النيابة العامة أمام المجالس القضائية، فيما يمثلها لدى المحكمة وكيل الجمهورية أو أحد مساعديه[2].

و تتولى النيابة العامة ممثلة في شخص وكيل الجمهورية إدارة نشاط الضبطية القضائية كما يتمتع هو نفسه بكافة السلطات و الصلاحيات المرتبطة بصفة ضابط شرطة قضائية، فيتولى مباشرة أو الأمر بمباشرة جميع الإجراءات اللازمة للبحث و التحري عن الجرائم بما في ذلك الجرائم المعلوماتية[3].

وله في حال مباشرة الإجراءات الخاصة بالبحث و التحري في الجرائم المعلوماتية حسب أحكام المادة 35 مكرر من قانون الإجراءات الجزائية المستحدثة بموجب الأمر 15–02 المؤرخ في 23 جويلية 2015، و مضمون الفقرة الأخيرة من (المادة 05 ق 04 – 09) المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و سبل مكافحتها، ان يستعين بمساعدين متخصصين في مجال المعلوماتية تحت مسؤوليته ،من أجل مساعدته في المسائل الفنية المتعلقة بالجريمة محل المتابعة، و ذلك بعد إطلاعهم على ملف الإجراءات المتخذة، و بعد أداءهم القسم المتعلق بالحفاظ على سرية المعلومات ،

---

[1]– المادة 29 قانون الإجراءات الجزائية الجزائري .

[2] – المادة 34 و 35 قانون الإجراءات الجزائية الجزائري.

[3] – المادة 36 قانون الإجراءات الجزائية الجزائري المعدلة بموجب الأمر 15–02 المؤرخ في 23 جويلية 2015.

و يقدمون اعمالهم في شكل تقارير تلخيصية او تحليلية تتضمن النتائج المتوصل إليها بناء على إلتماسات النيابة العامة ، و هو الإجراء الذي يهدف **حسب رأينا** إلى تحفيز أعضاء النيابة العامة على التعامل بصفة مباشرة مع الجرائم المعلوماتية من أجل إكتساب الخبرة و المهارات اللازمة في التعامل معها بصفة فورية و سريعة ،ربحا للوقت و عدم تفويت فرصة إحراز الأدلة في الوقت المناسب قبل إتلافها من قبل الجناة أو ضياعها نظرا لطابعها الإلكتروني ، بدل إصدار إتخاذ الأمر بإحالتها على الوحدات الخاصة بمكافحة الجرائم المعلوماتية و ما يترتب على ذلك من توفير فرصة للجاني في إتلاف الأدلة و محوها ، بسبب طول المدة بين وقوع الجريمة و ووقت إكتشافها و إنطلاق الإجراءات بشأنها.

ثانيا: اختصاص جهة التحقيق : يختص قاضي التحقيق بإجراءات البحث و التحري اختصاصا أصيلا حسب ما تقضي به المادة 38 – الأمر 69 – 75 قانون الإجراءات الجزائية الجزائري ، و يختص بالتحقيق في الجرائم إما بناء على طلب من وكيل الجمهورية أو شكوى مصحوبة بإدعاء مدني ضمن الشروط المنصوص عليها في (المادتين 67 و 73 من نفس القانون).

ووفق ما تنص عليه المادة 68 ق 01–08 من قانون الإجراءات الجزائية فإن قاضي التحقيق يقوم باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة بالتحري عن أدلة الإقناع و أدلة النفي، و إذا كان من المتعذر عليه القيام بها بنفسه جاز له أن ينيب و يندب ضابط الشرطة القضائية للقيام بتنفيذ جميع أعمال التحقيق اللازمة ضمن الشروط المنصوص عليها قانونا حسب المواد 138 إلى 192 قانون الإجراءات الجزائية، بما في ذلك الجرائم المعلوماتية، بما أن النص كان عاما و شاملا و لم يهدف بالتحديد و التخصيص لنوع الجرائم الجائز التحقيق فيها[1].

---

[1]– حسب ما تنص عليه الفقرة الأخيرة من (المادة 05 ق 04 – 09) المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و سبل مكافحتها فإن قاضي التحقيق و في حال توليه إجراءات التحقيق بنفسه بشان الجريمة المعلوماتية فله ان يستعين بكل شخص له دراية بعمل المنظومة المعلوماتية محل التفتيش بقصد مساعدته على إنجاز مهمته.

فإذن فالأشخاص المنوط بهم قانونا مباشرة أعمال التحري و التحقيق في الجرائم المعلوماتية هم ضابط الشرطة القضائية ، وكيل الجمهورية ، و قاضي التحقيق بحكم إختصاصهم النوعي، و كل شخص غير هؤلاء يتولى إجراءات البحث و التحري فإنه يعرض الإجراءات لطائلة البطلان المطلق نظرا لعدم إختصاصه النوعي.

و ما يلاحظ بهذا الشأن هو غياب دقة النصوص الإجرائية المحددة للإختصاص النوعي في مجال البحث و التحقيق في الجرائم المعلوماتية ، و هو ما يعني تضييق دائرة الاختصاص النوعي في مجال الجرائم المعلوماتية و حصرها في نفس مجال الجرائم العادية، بالرغم من تخصيص فرق للبحث و التحقيق في الجرائم المعلوماتية ، و هو ما من شأنه تعطيل عمل هذه الجهات و إحتمال تضييع أثار الجريمة نظرا لطبيعة الدلائل الالكترونية التي يمكن محوها و تدميرها في وقت قياسي، فلا حبذ لو اعاد المشرع النظر في مسألة تحديد الإختصاص النوعي في مسائل البحث و التحقيق في الجرائم المعلوماتية من خلال إفرادها بنصوص خاصة غير تلك المتعلقة بباقي الجرائم الأخرى ، بحيث يضمن النص سرعة التدخل ، بعيدا عن إجراءات طلب الإذن لأن طبيعة الجريمة المعلوماتية من حيث سرعة تنفيذها ، و محو أدلتها و أثارها لا تتناسب و طول مدة إستيفاء الشروط الإجرائية التقليدية ، مما يخلق فراغا إجرائيا بين النص و الجريمة و يتسبب في تعطيل الإجراءات و إفلات الجاني من العقاب .

الفقرة الرابعة: الاختصاص الإقليمي في مجال الجرائم المعلوماتية.

تعتبر الجريمة المعلوماتية نوعا خاصا من الجرائم فهي لا تعترف بمبدأ الإقليمية و لا بالحدود الجغرافية، فهي بمفهومها و طابعها الدولي قد قبلت مفاهيم الاختصاص الاقليمي للنص الجنائي و كذلك الإجرائي، فهي قد تقع في آن واحد و على مستوى عدة دول، و ذلك بسبب الطابع اللامادي للمعلومات و للمعطيات محل الجريمة، الذي نتج عنه مبدأ عدم اشتراط وقوع الجريمة المعلوماتية ضمن نطاق

الاختصاص الإقليمي للنص الجنائي حتى ينشأ الحق في المتابعة و التحقيق، و هي كلها معطيات أثارت إشكاليات ماسة بالمسائل الإجرائية[1].

و من الشروط التي يجب أن تتوفر في المحقق في الجرائم التقليدية صفة الإختصاص المكاني، أي أن لا يمارس إجراءات البحث و التحقيق خارج دائرة الاختصاص المكاني، و قد يمتد التحقيق في جريمة ما إلى ما خارج دائرة الاختصاص وفق ما يستلزم من ظروف التحقيق و مقتضياته، و تبقي بذلك الإجراءات صحيحة لا بطلان فيها.

إن إعمال الشروط التقليدية لقاعدة الاختصاص المكاني أمر لا مفر منه من أجل البحث و التحقيق في مجال الجريمة المعلوماتية، لكن كل ذلك غير كاف نظرا للطابع المميز لها، فهي بذلك تثير إشكالات عدة تجعل من اختصاص المحقق مكانيا غير مجد، نظرا لوجود محل البحث و التحقيق خارج نطاق الإختصاص الإقليمي المكلف به، كما سبق و أن وضحناه في المبحث الأول من الفصل الثاني، و هو ما سنعيد توضيحه بإيجاز في النقاط التالية:

أولا: قاعدة الاختصاص المكاني في الجرائم المعلوماتية على المستوى الداخلي.

1 – يمارس عادة وفق أحكام الفقرة 01 و 02 من المادة 16 ق 06-22 من قانون الإجراءات الجزائية الجزائري، ضابط الشرطة القضائية أعمال البحث و التحري ضمن اختصاصهم المحلي المحدد وقف الحدود التي يباشرون فيها وظائفهم العادية، و في حالة الاستعجال يباشرون مهامهم في دائرة اختصاص المجلس القضائي الملحقين به، و في حالة قدم لهم قاضي التحقيق المختص ضمن حالة الاستعجال طلب مباشرة أعمال البحث و التحري على المستوى الوطني فلهم ذلك، أما بالنسبة للجريمة المعلوماتية

[1]– Myriam Quéméner- Yves Charpenel – La Cybercriminalité – op.cit- p 159.

و وفق ما تنص عليه الفقرة الرابعة من نفس المادة ، فإن عمل و اختصاص ضابط الشرطة القضائية يمتد على مستوى الإقليم الوطني من أجل متابعة أعمال البحث و المعاينة، وذلك تحت إشراف النائب العام لدى المجلس القضائي المختص إقليميا ، مع إعلام و كيل الجمهورية المختص إقليميا.

2- بالنسبة لوكيل الجمهورية فإن إختصاصه الإقليم محدد وفق النطاق الإقبيمي لإختصاص الأقطاب المتخصصة ، و ذلك وفق ما تفرضه قواعد المرسوم التنقيذي 06-348 المؤرخ في 05 لأكتوبر 2006 ، و المعدل و المتمم بموجب المرسوم التنفيذي رقم 16 -267 المؤرخ في 17 أكتوبر 2016، إذن فنطاق إختصاصه إقليمي في مجال أعمال البحث و التحري في الجرائم المعلوماتية.

3- بالنسبة لقاضي التحقيق تجوز له حسب نص الفقرة الثالثة و الرابعة من المادة 47 ق 06-22 من قانون الإجراءات الجزائية أن يباشر عمليات التفتيش و الحجز ليلا او نهارا و في أي مكان على إمتداد التراب الوطني إذا ما تعلق الأمر بالجرائم المعلوماتية ، و هو ما يعني بالضرورة ان إختصاص كل من وكيل الجمهورية و قاضي التحقيق الإقليمي إذا ما تعلق الأمر بالجرائم المعلوماتية هو إختصاص وطني.

و في مجال تمديد الاختصاص الإقليمي دون عناء التنقل إلى مكان تنفيذ الإجراءات، أجاز القانون ما يعرف بالتفتيش عن بعد و الذي ينطوي على الدخول إلى المنظومة المعلوماتية محل التفتيش أو منظومة معلوماتية أخرى يمكن الدخول غليها إنطلاقا من المنظومة الأولى، تحتوي على المعطيات المبحوث عنها ، و ذلك من قبل السلطات القضائية المختصة و كذلك، ضباط الشرطة القضائية بعد إعلام السلطة القضائية (الفقرة 02 - المادة 05 - القانون 09 - 04 المتعلق بمكافحة الجرائم المعلوماتية)، و هو الإجراء الذي يسمح بربح الوقت و الجهد من خلال إختصار الإجراءات المتعلقة بتمديد نطاق الإختصاص و تعويضه بإجراءات ذات طابع تقني و فني تهدف إلى إحراز الأدلة بأسرع وقت ممكن .

ثانيا: قاعدة الاختصاص المكاني في الجرائم المعلوماتية على المستوى الخارجي.

بالنظر إلى الطابع الدولي للجريمة المعلوماتية فإن أعمال البحث التحقيق قد تستلزم تعدي نطاق الاختصاص الإقليمي الوطني لتمتد إلى إقليم دولة أخرى، و قد سبق و أن فصلنا في هذه النقطة بمناسبة المطلب الثاني من المبحث الأول من الفصل الثاني لبحثنا، فإن القواعد الخاصة المتبعة في سبيل ضمان شرعية الإجراءات هي الالتجاء إلى قواعد التعاون الدولي لمكافحة الجرائم المعلوماتية، فإذا تبين أن المعطيات المبحوث عنها و التي يمكن الدخول إليها من المنظومة الأولى ، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني ،فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة و وفقا لمبدأ المعاملة بالمثل[1] .

و من أمثلة التشريعات المقارنة التي أقرت بذلك التشريع الهولندي في مادته 125 فقرة 01 على إمكانية إجراء التفتيش داخل الأنظمة المعلوماتية المتواجدة في دولة أخرى بشرط أن يكون هذا التدخل مؤقتا و يهدف إلى كشف بيانات ضرورية لإظهار الحقيقة [2].

إذن فما يمكن قوله في شأن أحكام الاختصاص النوعي و المكاني التي تحكم عمل الجهات المختصة بالبحث و التحقيق في الجرائم المعلوماتية على المستوى الوطني، هو أنه و بالرغم مما تحمله من ضمانات شرعية إجرائية ، كضمانات لحقوق وحريات الأفراد إلا أنها تبقى غير متكاملة من حيث مفهومها وأحكامها الواردة في ظل كل من قانون الإجراءات الجزاءات الجزائية وقانون مكافحة الجرائم المعلوماتية 09 – 04، الذي يحدد القواعد الخاصة بالتفتيش عن بعد دون مراعاة قواعد الإختصاص

---

[1]– راجع بشان ذلك الفقرة **03 المادة 05** و المواد **16 –17–18** قانون 09–04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال الوارد في الملحق رقم **:02**

[2] – نبيلة هبة هروال– مرجع سابق– ص 240.

الإقليمي المبينة في قانون الإجراءات الجزائية، هذا الأخير الذي يضع شروطا وقواعد عامة تطبق على جميع الجرائم بما فيها المعلوماتية، والتي حدد الإختصاص الإقليمي بشأنها على المستوى الوطني وبدون شرط إعلام السلطة القضائية، عكس القانون 09 – 04 الذي جعل من مسألة تحديد الإختصاص الإقليمي لأجل التفتيش عن بعد بضرورة إعلام السلطة القضائية، وهما إجراءات مختلفان إحداها تفتيش مادي منصوص عليه في قانون الإجراءات الجنائية والآخر تفتيش رقمي منصوص عليه في القانون رقم 09 – 04 وهو ما يفتح باب التعارض في تطبيق نص القانونين فإلى أي قانون نلتجئ أولا وبأيها نعمل بدءا؟ وهي كلها عوائق تشريعية تمنع رجال البحث والتحقيق من تأدية مهامهم بالسرعة المطلوبة في مواجهة الجرائم المعلوماتية وهو ما يمنح للجاني فرصة إتلاف الدليل والإفلات من العقاب.

الفرع الثاني: المهارات الفنية لرجال البحث والتحقيق المعلوماتي.

عند الحديث عن المهارات الفنية التي ينبغي أن يكتسبها المحقق في الجرائم المتعلقة بالمعلوماتية فإننا لا نقصد بها المهارات التقليدية التي يجب أن يتمتع بها المحقق فهي مهارات أساسية يفترض توافرها في المحقق بالضرورة، فمهارات التعامل مع مسرح الجريمة والتحفظ على الأدلة ومناقشة الشهود، تعتبر من أساسيات أعمال التحقيق الذي لا يتوقع أحد عدم توافرها لدى المحقق، ولذلك فالمهارات المقصودة عند رجال البحث والتحقيق المعلوماتي هي تلك المهارات التي تتسم بالحداثة في مجال تقنية المعلوماتي.[1]

فمن الصعوبات التي تواجه رجال البحث والتحقيق المعلوماتي مسألة عدم التخصص ونقص الخبرة بصفة عامة، وذلك فيما يتعلق بثقافة الحاسوب وجرائم المعلوماتية وكيفية التعامل معها، وذلك بالخصوص

[1]– حسين بن سعيد الغافري–" التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الأنترنت"– بحث منشور على الموقع الإلكتروني الرسمي للمركز العربي للبحوث القانونية و القضائية للجامعة العربية– ص 02. تاريخ التصفح 2012 /03/23 –الرابط الإلكتروني:

http://www.carjj.org/node/1376

في الدول العربية، نظرا لحداثة الإعتماد على النظم المعلوماتية مقارنة بأوروبا والولايات المتحدة والولايات المتحدة الأمريكية، إضافة إلى الوقت الذي يستغرقه بتشكيل أجهزة مكافحة هذه الجرائم الذي يعتبر بطيئا مقارنة بنسق إنتشار الجرائم المعلوماتية، وهي الفوارق التي ينعكس أثرها سلبا على قيمة إجراءات البحث والتحقيق ، وهو ما يستدعي تأهيل سلطات البحث والتحقيق لأجل التحكم في هذه الجرائم.[1]

إن إكتشاف هذه الجرائم والتوصل إلى فاعلها بملاحقتهم قضائيا لا يتطلب الإلمام بأصول البحث الجنائي وقواعد التحقيق القانونية فقط فهو أمر مفترض عملا بقاعدة الشرعية الإجرائية، ولكن يجب كذلك الإلمام بأصول التحقيق الجنائي الفني في الجرائم المعلوماتية من خلال إكتساب مهارات خاصة تسمح بإستيعاب تقنيات الحاسوب من حيث برامجه وكيفيات إختراقه، ومصطلحاته ونفسية الجناة على إعتبار أنهم فئة خاصة يتعين التعامل معهم بأسلوب خاص.[2]

فما هي يا ترى هذه المواصفات الخاصة التي تجعل من رجال البحث والتحقيق مختصين في مجال الجرائم المعلوماتية؟

الفقرة الأولى: ضرورة التعرف على المكونات المادية للنظم المعلوماتية وآليات عمل الشبكات.

يجب أن يحيط رجال البحث والتحقيق في مجال الجرائم المعلوماتية علما بالجانب النظري للنظم المعلوماتية، و ذلك من خلال معرفة الجوانب التالية :

أولا: المكونات المادية للحاسوب: يجب على المحقق التعرف على الشكل المعين للحواسيب وملحقاتها ومسمى كل منها، والهدف من إستخدامه، وذلك حتى يستطيع وضع إحتمالات توظيفه في المجال الإجرامي، فعدم معرفته بالمكونات المادية للحاسوب قد يؤدي به إلى إهمالها أو حتى إتلافها بدون قصد أو يتسبب في تدمير أو تعديل البيانات المخزنة عليه نتيجة الجهل به، بل يجب عليه أن يلم بكيفية

---

[1] – عبد الفتاح بيومي حجازي– الجوانب الإجرائية لأعمال البحث والتحقيق الإبتدائي في الجرائم المعلوماتية– دراسة مقارنة على ضوء القواعد العامة للإجراءات الجنائية– الطبعة الأولى– دار النهضة العربية– مصر– 2009– ص 81.

[2]– المرجع السابق – ص 83.

التعامل معها وملحقاتها كذلك بإعتبارها أدلة محتملة، وأن يحرص على عدم تعريضها لأي من المؤثرات الخارجية التي تؤدي إلى تدمير محتوياتها كالقوى المغناطيسية، وإكتساب هذه المهارات هو نتاج الدورات التدريبية كما هو الحال في الولايات المتحدة الأمريكية وكندا.[1]

ثانيا: أساسيات عمل شبكات الإتصال: يتوجب على رجال البحث والتحقيق الجنائي المعلوماتي معرفة آليات عمل الشبكات المتصلة بالحاسوب، وخصوصا شبكة الأنترنت بإعتبارها شبكة دولية تربط بين ملايير الحواسيب عبر العالم، فعليه أن يجيد التعامل والتحكم في مبادئ الإتصال الشبكي وأنواعه، وكيفية إنتقال البيانات من جهاز لآخر، ومبادئ البروتوكولات الرسمية الخاصة بالإتصال بالشبكة، وتبرز أهمية تحكم المحقق بمبادئ عمل الشبكات في كونها ضرورة لبناء تصور شامل عن كيفية إرتكاب الفعل الإجرامي المعلوماتي، إضافة إلى إعتراض البيانات أثناء إنتقالها عبر الشبكة والتجسس عليها وتحويل مسارها، كما أنها تمنحه أكثر من ذلك وهي إمكانية تتبع مصدر الإعتداء.[2]

الفقرة الثانية: تمييز أنظمة التشغيل الحاسوبية ومبادئ التعامل معها وشبكة الأنترنت.

لا يكفي أن يكون المحقق على علم بالمكونات المادية للحاسوب فقط ، حتى يستطيع القول بانه مؤهل للتحقيق في الجرائم المعلوماتية بل يجب عليه ان يحيط علما كذلك بكل الجوانب المنطقية للأنظمة الحاسوبية و يمكن إيجازها في :

أولا: تمييز أنظمة التشغيل الحاسوب ومبادئ التعامل معها: يجب يكون لدى المحقق على الأقل فهم مبدئي بأنواع الأنظمة التشغيلية لأجهزة الحاسوب وخصائص ومميزات كل نظام تشغيلي، وكذلك أنظمة حفظ ومعالجة البيانات والملفات التي تعتمد عليها، وذلك حتى يتمكن من المشاركة في متابعة وفحص

---

[1] – حسين بن سعيد الغافري– مرجع سابق– ص 02.

[2] – خالد عياد الحلبي– مرجع سابق– ص 186.

وتفتيش مسرح الجريمة فقد يجد نفسه أمام حتمية إتخاذ قرار صعب بعد المشاورة مع الخبير، وبدون المعرفة التقنية فإن هذا القرار سيكون بيد الخبير وحده، وأكثر أنظمة التشغيل شيوعا والتي يتدرب عليها رجال البحث والتحقيق هي: ويندوز – لينكيس.[1]

ثانيا: التعرف على الصيغ المختلفة لتطبيقات الحاسوب : يتوجب على المحقق كذلك أن تتوفر فيه صفة المعرفة بالصيغ المتنوعة لتطبيقات الحاسوب، وذلك ليصبح قادرا على معرفة مكان الملفات المخزنة وما تتضمنه من معطيات، كما يشترط معرفته لأهم التطبيقات التي تمكنه من قراءة أو مشاهدة محتوى هذه الملفات على أساس أنه ملف في غاية الأهمية، وبإعتبارها الوعاء الحقيقي لأدلة الإدانة لما تحتويه من معلومات في شكل رقمي محفوظة على شكل ملفات، يتميز كل ملف ببينة وصيغة خاصة تميزه عن غيره.

ثالثا: التعامل بالشكل الصحيح مع شبكة الأنترنت : يعتبر الأنترنت أداة تحري مناسبة لرجال البحث والتحقيق المعلوماتي، فهي تسمح لهم توضيح غموض بعض الجرائم ، فمن الضروري إستخدامها حتى يستطيع التصدي لها من خلال تبادل الملفات ونقل الرسائل الإلكترونية كما تتيح لهم الإطلاع على مستجدات جرائم المعلوماتية وطرق مكافحتها.[2]

الفقرة الثالثة: ضرورة معرفة الأساليب الإجرامية في مجال المعلوماتية.

معرفة رجال البحث والتحقيق بأساليب إرتكاب الجرائم المعلوماتية أمر غاية في الأهمية خاصة، فهي تساعدهم على معرفة طبيعية المجرم، والموقع الإحتمالي لإرتكاب الجريمة، كما تساعد من يتولى مسائل مناقشة الشهود واستجواب المتهمين في طرح الأسئلة المباشرة المتصلة بالسلوك الإجرامي، كما أنها

---

[1] – حسين بن سعيد الغافري– مرجع سابق– ص 03.

[2] – خالد عياد الحلبي– مرجع سابق– ص 187، 188.

تساعد المحقق على التواصل مع خبير الحاسوب، عند شرح هذا الأخير لما توصل إليه من أدلة وقرائن، والأساليب المستخدمة في إرتكاب الجريمة والأدوات المستعملة في ذلك.[1]

كما أن الإلمام بتقنيات الأمن المعلوماتي من الأمور المهمة التي لا بد من معرفتها من قبل المحقق، فمعرفتها واستعمالاتها تساعده ميدانيا في عمله، فعندما يباشر تحقيقا في جريمة إختراق نظام معلوماتي في لشركة أو مؤسسة فهو يسأل القائمين على نظامها المعلوماتي عن نوع البرامج الحمائية والأمنية المستخدمة وكيفية عملها وهو ما يسمح له بإستخلاص الوصفة التفاعلية بينها وبين الفعل الإجرامي، من خلال ما يرد في التقارير التي يعدها الخبير من خلال قراءة أنظمة تقنية الجدار الناري (Fire wall) ونظام الخادم الوكيل (Proxy server).[2]

الفرع الثالث: ضرورة الخضوع لدورات تدريبية وتكوينية في مجال المعلوماتية.

إضافة إلى جملة المعارف التي يشترط ان يحيط بها المحقق علما من أجل أن يكون مؤهلا لمباشرة أعمال البحث و التحقيق في شان الجرائم المعلوماتية ، فإنه لا بد ان يكون محل تكوين نظري و تدريب عملي مستمر و دائم و ذلك كنتيجة حتمية لطابع التطور المستمر للجريمة المعلوماتية ، و للتدريب أهمية و منهج خاص نبينه فيما يلي :

الفقرة الأولى : أهمية التدريب في مجال مواجهة الجرائم المعلوماتية.

التدريب والتكوين يعد جزءا من عملية التنمية الإدارية، فهو يهدف بالدرجة الأولى إلى زيادة الكفاءة والفعالية والقدرة على إنجاز العمل ومن ذلك فقد حرصت الكثير من المنظمات العامة والخاصة على

---

[1] – حسين بن سعيد الغافري – مرجع سابق – ص 05.

[2] – خالد عياد الحلبي– مرجع سابق– ص 190، و لمزيد من التفصيل حول مفهوم Proxy Server–Fire Wall– أنظر قاموس المصطلحات المعلوماتية– الملحق رقم : **01.**

العناية به، بإعتباره أحد الأدوات الرئيسية لرفع مستوى الأداء، والهدف من عملية التدريب إدخال واستحداث تعديلات جوهرية على سلوك المتدربين تكون أثارها واضحة في سلوكهم لأداء الأعمال التي يكلفون بإنجازها كل في مجال تخصصه بشكل أفضل بعد عملية التدريب لا قبلها.[1]

ويميل الفقه الجنائي إضافة إلى الواقع العملي إلى القول بأن التحقيق في مجال الجرائم المعلوماتية في حاجة إلى خبرة ومهارات خاصة لا تتأتى إلا بالتدريب المتخصص يراعي فيه عدة عناصر تتعلق بشخص المتدرب ومنهج التدريب ، فبخصوص المتدرب لا بد أن يكون مؤهلا لذلك سواء أكان من ضباط الشرطة القضائية أو سلطات التحقيق أو النيابة العامة، فيجب أن تتوافر فيه قدرات ذهنية ونفسية خاصة، غير أن تدريب المتخصص في معالجة البيانات ونظم التشغيل يؤتي ثماره بسرعة مقارنة بأولئك المنتمين لسلك الشرطة أو العدالة.[2]

كما يشترط كذلك في المتدرب أن يكون على قدر من الخبرة، فقد ذهب بعض الخبراء إلى تحديد شرط 05 سنوات في المجالات ذات العلاقة بتكنولوجيا المعلومات من أجل وضع الشخص ضمن قائمة المتدربين.[3]

أما بالنسبة للمنهج التدريبي فيجب أن يتضمن المحتوى الجوانب التالية:

- الواقع الحالي والإتجاهات المستقبلية للجرائم المعلوماتية، ومن أجل التعرف على الفئات المختلفة التي ينقسم إليها مجرمو المعلوماتية.

---

[1] – يوسف حسن يوسف– مرجع سابق ص 176.

[2] – عبد الفتاح بيومي حجازي– الجوانب الإجرائية لأعمال البحث والتحقيق الإبتدائي في الجرائم المعلوماتية– دراسة مقارنة على ضوء القواعد العامة للإجراءات الجنائية – مرجع سابق– ص 89

[3] – يوسف حسن يوسف– مرجع سابق– ص 177.

- الجانب التشريعي من أجل فهم ومعرفة الشيء القانوني المتعلق بهذه الجرائم والإلمام بإتجاهات القوانين والتشريعات.
- دراسة وتحليل القضايا المشهورة للإستفادة من تجارب العدالة في مواجهة هذه الجرائم.
- الوقوف على الأبعاد الدولية وآليات التعاون المشترك بين الدول والتعرف على الإتفاقيات والمعاهدات الدولية.[1]

الفقرة الثانية : المحاكاة الحاسوبية كأسلوب تدريب ملائم في مجال الجرائم المعلوماتية.

إن ما يجب الإشارة إليه في هذا الصدد هو تقنيات التدريب المعروفة بإسم المحاكاة الحاسوبية التي تعرف بأنها تقليد محكم يطابق ويماثل الأصل تماما، بحيث يتم التعايش مع ظروف وملابسات وإحتمالات الواقع العملي للمواقف والأحداث بصورة تزيد من القدرة على التعامل مع هذه المواقف في الحياة العملية.[2]

إن إتباع الأسلوب التدريبي سيؤدي إلى إكتساب الأفراد العاملين في مجال البحث والتحقيق المعلوماتي وفي حالة الإعداد الجيد للنموذج المحاكي للواقع الميداني لعملهم، لمعارف وإتجاهات ومهارات مرتبطة بكيفية أداء العمل واستخلاص النتائج والربط بينها وكيفية التصرف في موقف محدد بأعلى قدرة من الفعالية.[3]

إذن فمسألة الإختصاص في مجال أعمال البحث والتحقيق المعلوماتي ليست مسألة ذات طابع قانوني، بل هي أوسع من ذلك لتمتد إلى شروط الإختصاص الفني والعلمي بمجال النظم المعلوماتية، فبدونها

---

[1] – حسين بن سعيد الغافري– مرجع سابق– ص 03.

[2] –ممدوح عبد الحميد عبد المطلب– البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت– دار الكتب القانونية– مصر– 2007– ص 150.

[3] – ممدوح عبد الحميد عبد المطلب– مرجع سابق– ص 174.

لا يمكن مباشرة أعمال البحث والتحقيق من قبل الجهات المختصة ولو استوفت شروط الإختصاص النوعي والإقليمي، نظرا لما تطرحه غياب ثقافة التعامل مع النظم المعلوماتية، من إشكاليات عملية، وهو الأمر الذي لم يستدركه بعد التشريع الجزائري وفق نصوص قانون الإجراءات الجزائية، وترك أمر تنظيمه للقوانين الخاصة بأسلاك الأمن الوطني والدرك الوطني اللتان تبذلان مجهودات معتبرة في هذا المجال من أجل التكييف مع الواقع الحديث للإجرام، وذلك من خلال عزمها على تعميم الفرق المختصة بمكافحة الجرائم المعلوماتية على المستوى الوطني مع تجهيزها بأحدث التقنيات والعمل على رفع كفاءة موظفيها من خلال تكوينهم الدائم والمستمر في الدول التي أحرزت تقدما ملحوظا في هذا المجال.

المطلب الثاني: الإجراءات الخاصة بالبحث و التحري في جرائم المعلوماتية.

الجريمة المعلوماتية وكغيرها من أنواع الجرائم الأخرى، تمر بذات مرحلتي الإستدلال والتحقيق القضائي، وما يترتب على ذلك من إجراءات قانونية وفنية وشكلية ويعتبر إجراء التحقيق القضائي، هو الأساس في مجال البحث والتحقيق المعلوماتي، وذلك لما يكتسبه هذا الأخير من أهمية قصوى في مجال إستخلاص الحقائق بشأن الجريمة، لكن تبقى الإجراءات الأخرى الخاصة بمرحلة الإستدلال أو التحري الفنية منها خصوصا ضرورية لأجل إستكمال متطلبات التحقيق القضائي في مجال الجريمة المعلوماتية.[1]

يختص ضباط الشرطة القضائية بمسألة التحري بشأن الجرائم التقليدية والمعلوماتية على حد سواء، وتختلف طرق مواجهة كل منها، فالأخيرة تتميز بطبيعة خاصة إذ أن أدلتها غير محسوسة ويحتاج أمر التحري بشأنها إلى خبرات قضائية فنية وتقنية عالية، وذلك على مستويين:

---

[1] – عبد الفتاح بيومي حجازي– الجوانب الإجرائية لأعمال البحث والتحقيق الإبتدائي في الجرائم المعلوماتية– دراسة مقارنة على ضوء القواعد العامة للإجراءات الجنائية – مرجع سابق– ص 67.

- التحري عن الجرائم المعلوماتية قبل وقوعها، وذلك من خلال تبني تكتيك المراقبة الدورية للشبكات والنظم المعلوماتية، وكذلك مراقبة أعمال مقاهي الأنترنت للحيلولة دون وقوع إعتداءات معلوماتية.
- التحري عن الجرائم المعلوماتية بعد وقوعها أي إتخاذ كل الإجراءات التي تخص معاينة مسرح الجريمة من أجل إحراز الدليل الواضح والذي يمكنهم من نسبة الجريمة إلى فاعلها.

تتجلى الصعوبة في هذا الخصوص في حال وقوع الجريمة على برامج الحاسوب أو بواسطة شبكة الأنترنت، ففي هذه الحالة يواجه ضباط الشرطة القضائية إشكالية فقدان الأثار بسبب إمكانية محوها أو تدميرها في مدة قصيرة من قبل أي شخص يتردد على مكان الجريمة، فما هي يا ترى الإجراءات التي تتخذها الجهات الخاصة بمهام البحث والتحري بشأن الجرائم المعلوماتية والتي تسمح لهم بتحصيل الدليل؟

سنحاول الإجابة عن هذه الإشكالية من خلال تعرضنا للمسائل التالية وهي مسائل الكشف عن الجرائم والتبليغ عنها (الفرع الأول) ،الإجراءات الخاصة المتبعة التي يجب إتخاذها قبل الإنتقال لمعاينة مسرح الجريمة (الفرع الثاني)، وأخيرا نتعرض لمسؤولية مزودي الخدمة بالأنترنت في مجال التعاون مع جهات البحث والتحري (الفرع الثالث).

الفرع الأول: آليات الكشف والتبليغ عن الجرائم المعلوماتية.

كما سبق و ان فصلنا بشأن خصوصيات الجريمة المعلوماتية ، فقد أكدنا على طابعها الخفي فهي نادرا ما تكون تحت وصف حالة التلبس إن لم نقل أن ذلك امر مستحيل ، فالمجرم المعلوماتي يبذل كل ما في وسعه للإبقاء على جريمته خفية ، و ما يجعل من امر كشفها و التبليغ لاحقا عنها ، فما هي آليات الكشف عن هذه الجرائم ، و كيف يتم التبيلغ و التعامل مع التبليغات بشأنها من قبل الجهات المختصة؟

الفقرة الأولى: آليات الكشف عن الجرائم المعلوماتية.

إن الإشكال الذي يواجه أجهزة الأمن والمحققين من رجال الضبطية القضائية، هو أن الجرائم المعلوماتية لا تصل إلى علم السلطات المعنية بالصور العادية، وذلك الصعوبة إكتشافها من قبل الأشخاص العاديين وحتى المؤسسات والشركات لا تكتشف هذه الجرائم فور وقوعها على إعتبار أن أغلبها لا يراجع حساباته بشكل يومي، وحتى وإن تم ذلك بشكل يومي أو شهري فإنه يصعب عليها التأكد من الفوارق في الأرقام التي تبدو عادة خسائر أو ديون أو حتى في حال إكتشافها فإن أغلب تلك الشركات تتردد في التبليغ خوفا على سمعتها.[1]

وهنا تظهر أهمية دور الأجهزة الأمنية في رصد حركة مرتكبي جرائم المعلوماتية وإكتشاف هذه الجرائم من خلال الرصد الميداني لحركة المعاملات التجارية ومراقبة المشبوهين داخل المؤسسات المالية وحولها، فالقدرة على الملاحظة وقراءة تصرفات الأشخاص العاملين في مجال المعلوماتية، والمهتمين بالبرامج، وهواة صناعة الأنظمة هي أولى خطوات السيطرة الأمنية على نشاط مرتكبي جرائم الحاسوب ويتعزز كل ذلك من خلال تكثيف المراقبة من قبل الوحدات الخاصة لمكافحة الجريمة المعلوماتية في الأماكن وحول الفئات التالية:

- أسواق أجهزة الحواسيب والبرامج المعلوماتية.
- الرصد الدقيق لحركة المترددين على المواقع المذكورة أعلاه.
- الرصد الدقيق لحركة المشبوهين في مجال جرائم الأموال وتجار المخدرات.
- الرصد الدقيق لحركة معتادي جرائم التزوير و الإحتيال و معتادي الإجرام المعلوماتي.

---

[1] – ضياء علي أحمد النعمان– مرجع سابق– ص 364.

إن هذا القدر من التواجد الميداني المنظم يضمن تغطية أمنية على منافذ المعلومات والحاسوب وله أثر وقائي ورادع في نفس الوقت، كما يسمح بتوفير المعلومات الأولية عن الجرائم المعلوماتية قبل وقوعها كما يضمن سرعة التبليغ عنها وإتخاذ الإجراءات بحقها.[1]

الفقرة الثانية: كيفية التعامل مع التبليغ بشأن الجرائم المعلوماتية.

البلاغ هو إخطار السلطات المختصة بوقوع جريمة، وهذا الإخطار واجب أدبي يتقيد به المواطن الصالح سواء وقعت الجريمة عليه أو على غيره ، إن أهمية التبليغ تعطي للمجني عليه ولغيره من الأفراد في الجرائم المعلوماتية دور لا يستهان به لأنه قد يكون السبيل الوحيد لكشف هذه الجرائم، وهو دور يعطي الفرصة لأجهزة الضبطية القضائية فرصة التحرك بسرعة من أجل مواجهة الجريمة المعلوماتية ويعتبر عدم الإبلاغ سببا رئيسيا في تفاقم الجرائم المعلوماتية.[2]

فالتبليغ هو المشكلة الحقيقية التي الجهات المختصة بمواجهة الجريمة المعلوماتية ، فغالبية الهيئات فالمؤسسات تخشى الإبلاغ عن الجرائم المعلوماتية خوفا من فقدان عملائها وهو ما ينتج عنه إفلات مرتكب الجريمة بفعلته.[3]

والتبليغ هو إخبار السلطات المختصة عن وقوع جريمة، أو أنها على وشك الوقوع ، أو كان هناك إتفاقا جنائيا، أو أدلة أو قرائن أو عزما على إرتكابها، أو وجود شك أو خوف من أنها ارتكبت.[4]

---

[1] – عبد الفتاح بيومي حجازي– الجوانب الإجرائية لأعمال البحث والتحقيق الإبتدائي في الجرائم المعلوماتية– دراسة مقارنة على ضوء القواعد العامة للإجراءات الجنائية– مرجع سابق– ص 72 – 75.

[2] – خالد عياد الحلبي– مرجع سابق– ص 192.

[3] – عبد الله بن سعود بن محمد السراني– مرجع سابق– ص 67.

[4] – نبيلة هبة هروال– مرجع سابق– ص 177.

وفي هذا الصدد نصت الفقرة الأولى من المادة 17 المعدلة بموجب الأمر 15-02 من قانون الإجراءات الجزائية الجزائري على أنه " يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 12و 13 و يتلقون الشكاوى و البلاغات و يقومون بجمع الإستدلالات و إجراء التحقيقات الإبتدائية " تقابلها نص المادة 17 من قانون الإجراءات الجزائية الفرنسي والمادة 24 من نظيره المصري و 27 من نظام الإجراءات الجزائية السعودي.

والتبليغ عن الوقائع الجنائية حق لكل شخص بل هو واجب مفروض عليه فلا يصبح معاقبته وإقتضاء التعويض منه، إلا إذا تعمد الكذب، وتوافرت في شأنه أركان جريمة البلاغ الكاذب.[1]

ويتكفل ضباط الشرطة القضائية بتلقي البلاغات ومباشرة الإجراءات المتعلقة بالتحقيقات الإبتدائية، ولهم الحق في سبيل ذلك طلب مساعدة القوة العمومية أثناء تنفيذ مهامهم، وتختم أعمالهم بإعداد محاضر ترسل إلى وكيل الجمهورية لأجل إخطاره بالجنح والجنايات التي تصل إلى عملهم.[2]

ويستحب أن يكون المبلغ في الجريمة المعلوماتية على درجة مقبولة من الإلمام والمعرفة بالجوانب الفنية للحاسوب، حتى يتمكن من تقديم معلومات تصف الحادث بالشكل الذي يمكن معه لضباط الشرطة القضائية من مباشرة البحث والتحري عنها، وهو ما يستلزم أن يكون متلقي البلاغات على قدر من المعرفة بالجوانب المعلوماتية، حتى سيضع مناقشة المبلغ في الكثير من جوانب الجريمة محل البلاغ.[3]

و يتم التبليغ باعتباره أولى خطوات إجراءات البحث و التحقيق المعلوماتي من خلال:

---

[1] – راجع المواد: 91 و92 من قانون العقوبات الجزائري.

[2] – المادة 17 المعدلة بموجب الأمر 15-02 و المادة 18 من قانون الإجراءات الجزائية الجزائري

[3] – خالد عياد الحلبي- مرجع سابق- ص 193.

- تلقي جهات الضبطية القضائية معلومات أمنية تشير إلى ممارسته شخص معروف أو غير معروف أنشطة معلوماتية محظورة.
- توفر معلومات عن انتشار الفيروسات التخريبية عبر شبكة الإنترنت.
- ضبط شخص بحيازة مستندات أو محررات مزورة أو بطاقات ائتمان مزورة.[1]

الفقرة الثالثة : كيفية التبليغ عن الجرائم المعلوماتية.

إن التبليغ عن جرائم المعلوماتية لا يختلف عما هو عليه الحال في مجال الجرائم التقليدية ، غير أنه يتمتع بنوع من الخصوصية يتماشى و طبيعة هذه الجرائم ، فالبلاغ في هذه الحالة قد يتم عن طريق شبكة الأنترنت أو ما يعرف بالبلاغ الإلكتروني ،وذلك بإطلاع الهيئات المختصة بالبحث و التحري بواسطة رسالة إلكترونية عن وجود أعمال غير مشروعة ،أو عن موقع ينشر صورا جنسية للأطفال هو ما يوفره البريد الإلكتروني للدرك الفرنسي من خلال البريد الإلكتروني: judiciare@gendaremeriedefense.gov.fr بإعتباره الجهة المختصة بالتحري و التحقيق في شأن هذه الجرائم في فرنسا، و كذلك الحال في مصر من خلال الإتصال بموقع شرطة إدارة مكافحة جرائم الحاسب و شبكات المعلومات في مصر.

قد يكون التبليغ من خلال ملئ المبلغ لإستمارة رقمية على الموقع المخصص لتلقي البلاغات و الشكاوي كذلك التى يوفرها الموقع الرسمي لأنترنت الأحداث www.intrenet.miners.gov.fr في فرنسا ،أو تلك المتوفرة على موقع إدارة مكافحة جرائم الحاسبات و شبكات المعلومات المصري على الرابط التالي:www.ccd.gov.eg[2]

---

[1] – عبد الله بن سعود محمد السراني– مرجع سابق– ص 182 – 183.

[2] – نبيلة هبة هروال– مرجع سابق– ص 182 – 183.

وهي الإمكانية المتاحة على المستوى الوطني من خلال إمكانية التبليغ التي تتيحها المواقع الخاصة بالجهات الأمنية كجهاز الشرطة والدرك الوطني، هذا الأخير الذي يضع تحت تصرف المواطنين البريد الإلكتروني لأجل التواصل مع هذه الجهات والتبليغ عن كافة الجرائم والجرائم المعلوماتية، وذلك عبر البريد الإلكتروني من خلال العنوان الإلكتروني : ccom-cgn@mdn_dz ، او من خلال الخدمة التي أصبحت متاحة منذ 07 أفريل 2015 المتعلقة بإيداع الشكاوى أو المعلومات المتعلقة بالجرائم عبر الموقع الألكتروني المستحدث من قبل هيئة الدرك الوطني على العنوان التالي : https://ppgn.mdn.dz ، و هو مايوفره كذلك موقع المديرية العامة للامن الوطني على موقعه www.dgsn.dz الذي يمكن لأي شخص من التبليغ وبصفة تضمن سرية هويته ، عن اي جنحة او جناية وذلك بهدف تشجيع الغير على التبليغ عن الجرائم بما فيها المعلوماتية ، ويبقى للمبلغ حرية الإختيار في الأخير بين الأسلوب التقليدي أو الإلكتروني .

وتظهر أهمية تلقي البلاغات في أنها تساعد رجال البحث والتحري على تحديد نوع الجريمة المبلغ عنها ان كانت تندرج ضمن الجرائم المعلوماتية ، و كذلك وضع تصور مبدئي لخطة العمل المناسبة للبحث والتحري بشأن الجريمة، و بالتالي تحديد نوع الخبرة المطلوبة لأجل المعاينة وتحريز الأدلة وما يجب التأكيد عليه ان جهة تلقي البلاغ يجب عليها ان تحرص على ان يقوم المبلغ بالخطوات التالية:

- تجهيز قائمة بأسماء العاملين في المؤسسة أو المشتبه فيهم .
- تجهيز نسخة إحتياطية من بيانات الأجهزة المتضررة.
- عدم تبليغ أي أحد آخر بالجريمة الواقعة.[1]

---

[1] - خالد عياد الحلبي- مرجع سابق- ص 195.

الفرع الثاني: وضع خطة وتكوين فريق العمل.

إن أمر تقصي الحقيقة و تتبع الدليل الإلكتروني الناتج عن الجريمة المعلوماتية ، يحتاج إلى تضافر الجهود ، من اجل الإحاطة بكل جوانب الجريمة من القانونية إلى المعلوماتية إلى تلك الفنية ، و هو ما يستدعي تشكيل فريق من المختصين كل في مجاله لأجل التكفل بمهام البحث و التحقيق المعلوماتي ، و ذلك و فق خطة محددة مسبقا تهدف إلى تنظيم العمل و تحقيق الهدف المنشود ، و سنحاول إبراز كل ذلك في الفقرات اللاحقة .

الفقرة الأولى: وضع خطة العمل.

بعد الإنتهاء من جمع المعلومات الأولية المتعلقة بالجريمة المبلغ عنها، أو تلك محل الشكوى، يبدأ رجال البحث والتحري بناء على ضوء المعطيات المستقاة بتحديد خطة العمل المناسبة وتشكيل فريق العمل اللازم للتحري في الحادثة، وهذه الخطة يجب أن تكون قد اكتملت في ذهن المحقق بمجرد إنتهاءه من أخذ الإفادة من المبلغ أو الضحية واتضحت لديه الصورة الأولية عن الحادثة الجرمية قبل التنقل إلى مسرح الجريمة لأجل مباشرة إجراءات المعاينة والضبط وذلك من خلال الإرتكاز على النقاط التالية:[1]

- تحديد حجم الجريمة محل البحث والتي تحدد حجم ونوع الفريق اللازم للتدخل فجرائم المعلوماتية تتنوع مابين بسيطة ومعقدة وذلك حسب طبيعتها الفنية الخاصة، التي تفرض على أعضاء فريق التحقيق إمتلاك مهارات فنية خاصة وضرورية للتعامل معها.
- تحديد الظروف المحيطة بالجريمة و بالخصوص:
  - مدى أهمية محل الجريمة ومدى نسبة الضرر التي لحقت بالضحية.

---

[1] – علي عدنان الفيل – مرجع سابق– ص 13.

- مدى تضرر الأجهزة الحاسوبية والشبكات.
- إعداد قائمة بأسماء المتهمين المحتملين.
- تحديد مستوى الإختراق الأمني الذي يتسبب فيه الجاني.
- تحديد مستوى مهارة المجرم المعلوماتي.
- تحديد طبيعة مسرح الجريمة والأسلوب الأمثل للتعامل معها، وهذه النقطة مهمة جدا وإخفاق المحقق في تحديد طبيعة الأسلوب المناسب للتعامل مع الجريمة قد يؤدي إلى عدم الحصول على أية نتيجة أو الحصول على كم هائل من النتائج بدون فائدة.[1]

- مراعاة الضوابط القانونية فالإجراءات المسبقة التحديد تساعد على ضمان أن الخطوات التي يقوم بها المحقق خلال جميع مراحل البحث تتم وفق ضوابط إجرائية شرعية ولا تعرض الإجراءات لطائلة البطلان في مراحل متقدمة من سير الدعوى.[2]
- تعيين الأشخاص الذين سيتم إستجوابهم وتحديد الأسئلة والنقاط التي يجب إستيضاحهم بشأنها وكذلك تقدير مدى الحاجة إلى الإستعانة بأصحاب الخبرة والإختصاص التي يفتقدها فريق التحقيق.[3]

بعد وضع الخطة يشترط كذلك وبصفة آلية تعيين فريق التحقيق وتشكيله من أجل مباشرة الأعمال المتعلقة بالتحري والبحث في مدى صحة البلاغات والشكاوي الواردة بشأن الجريمة المعلوماتية.

الفقرة الثانية: تشكيل فريق العمل.

يجب وفي مجال البحث والتحري بشأن الجرائم المعلوماتية، تشكيل فريق تحقيق يمزج بين الخبرة في مجال البحث والتحري في الجرائم العادية، وبين التخصص في مجال المعلوماتية، فهناك عادة محققون

---

[1] – حسين بن سعيد الغافري– مرجع سابق– ص 07.

[2] – خالد عياد الحلبي– مرجع سابق– ص 198.

[3] – علي عدنان الفيل– مرجع سابق– ص 16.

دور خبرة طويلة في مجال البحث الجنائي، و هناك أخصائيون في مجال المعلوماتية ذوي معرفة واسعة، ولكن من النادر أن يوجد محقق تتوفر فيه الصفتين معا، لا سيما وأن عالم المعلوماتية متشعب وعلى درجة كبيرة من التعقيد ولذلك وجب أن يتضمن فريق العمل في مجال التحري والبحث خبراء وفنيين من هذا المجال، وذلك حسب ما تفرضه وقائع كل قضية، كما أن فريق التحقيق قد يتطلب الإستعانة ببعض خبراء مسرح الجرائم التقليدية كخبير البصمات و ممن ليس لهم دور وثيق الصلة بالطبيعة الخاصة بجرائم المعلوماتية غير أنه لا يتصور خلو أي فريق منهم نظرا لما يحققونه من فائدة من خلال أدوارهم الثانوية[1]، وعلى كل حال فإن فريق العمل يجب أن يتكون من:

أولا: المشرف على التحقيق: أو المحقق الرئيسي والذي يجب أن يكون من ذوي الخبرة الطويلة في مجال التحقيق الجنائي في الجرائم المعقدة، مع إلمامه بالجوانب المعلوماتية، ويتولى مهمة الإشراف على إدارة الفريق وتوزيع المهام على أعضاءه.[2]

ثانيا: فريق خبراء الحاسوب والشبكات: قد يضم شخصا واحدا وأكثر حسب ظروف الجريمة وهو شخص لديه خبرة ومعرفة بوسائل وأساليب لتحقيق وإجراءاته، مع إلمامه بطبيعة الجرائم المعلوماتية وكيفية التفتيش عن الأدلة الإلكترونية والتعامل معها وأخذ الإفادة من ذوي العلاقة مع مسرح الجريمة.[3]

ثالثا: خبراء تدقيق الحسابات الإلكترونية : هو شخص أو أكثر لديه إختصاص في مجال المراجعة المحاسبية على درجة عالية من الخبرة في التعامل مع البرمجيات المستخدمة، والآليات التي يتم بموجبها

---

[1] – حسين بن سعيد الغافري– مرجع سابق– ص 07.

[2] – عبد العال الدريبي– مرجع سابق– ص 310.

[3] – علي عدنان الفيل – مرجع سابق– ص 17.

تبادل الأموال إلكترونيا، ينصب عمله على تحديد أسلوب الجريمة وأساليب التلاعب بالأنظمة وتقدير الخسائر الناتجة عن الجريمة.

رابعا: فريق ضبط وتحريز الأدلة: يتكون هذا الفريق من خبراء رفع البصمات كإجراء عام في معظم الجرائم وذلك من خلال التركيز على المكونات المادية للحاسوب والشبكات المتضررة، أو المستعملة في الجريمة، وبالخصوص لوحة المفاتيح والقارة والشاشة والطابعة.[1]

خامسا: فريق الرسم والتصوير: يضم شخصا أو أكثر يقومون بتصوير أو رسم تخطيطي (كروكي) لمسرح الجريمة وتحديد موقع الأجهزة والملفات والأشخاص، وإلتقاط الصور الفتوغرافية والتصوير بالفيديو.

سادسا: فريق التفتيش العلمي: يتولى هذا الفريق عملية البحث الدقيق على مسرح الجريمة وفق النظم القانونية التي تتبع التفتيش في الأماكن، فيقومون بالمرور على كل الغرف والأماكن مع فحصها بشكل دقيق لأجل الكشف عن أشياء مخفية، ويستحب أن يكون هؤلاء من خبراء الحاسوب.

سابعا: فريق التأمين والقبض: توكل لهذا الفريق مهمة السيطرة الأمنية على مسرح الجريمة وضبط مداخلها ومخارجها وحركة الموجودين بها، والمباني المجاورة لها وتنفيذ عملية القبض على المشبه فيهم ويتكون عادة من رجال الأمن بالزي الرسمي[2].

ثامنا: الخبير الإستشاري: يعمل الخبير الإستشاري على تحقيق هدفين في مجال مساعدة فريق التحقيق المعلوماتي وهما:

---

[1] – حسين بن سعيد الغافري– مرجع سابق– ص 03.

[2] – عبد العال الدريبي– مرجع سابق– ص 310 ، 311.

- القيام بدور توضيحي للواقعة.
- إزالة الغموض عن وقائع معينة.

فمثلا في جرائم الأنترنت يكمن عملة في توضيح طريقة عمل شبكة الأنترنت ثم يطرح رأيه الخاص حول النقاط الغامضة المتعلقة بالجريمة، ما قد يحل إشكالا عالقا وعمله كخبير إستشاري هو ترجمة لمهاراته الفائقة التي قد لا تتوفر عند المحقق والخبير المعلوماتي.[1]

إذن تعتبر خطة العمل وتشكيلة فريق العمل من القيم الأساسية والثابثة في مجال البحث والتحقيق المعلوماتي، فأي محاولة لتتبع أثارها من دون التشكيل الضروري والخطة المناسبة سيكون مصيره الفشل لا محالة ،نظرا لسرعة تنفيذ الجريمة المعلوماتية وسهولة محو الدليل،وإعتمادها على أساليب قد تتعدى قدرة الفريق مجتمعا، وهو ما يستدعي ضرورة بقاء أفراده على إتصال دائم بعالم المعلوماتية لأجل تحصيل المستجدات،التي تمكنهم من الوصول إلى نتائج جد فعالة في مجال القبض على مجرمي المعلوماتية من خلال تعقبهم وملاحقتهم، و ذلك بإعتماد أساليب حديثة و متناسبة والجرائم المعلوماتية وهو ما سنحاول إستعراضه في الفرع التالي.

الفرع الثالث:الخطوات الأولية لمباشرة أعمال البحث والتحري عن الجرائم المعلوماتية.

تعتبر الجريمة المعلوماتية من قبيل الجرائم الخفية، أي أنها عبارة عن أنشطة إجرامية تتم في سرية بتخطيط وإعداد مسبق وتنفيذ بطريقة مدروسة من قبل مجرمين متمرسين في عالم الجريمة تجمعهم مصلحة عدم إبلاغ السلطات المختصة عن نشاطهم الإجرامي.[2]

---

[1] – خالد عياد الحلبي– مرجع سابق– ص 202.

[2]– محمد محمد محمد عنب– إستخدام التكنولوجيا الحديثة في الإثبات الجنائي– دون ذكر دار النشر– مصر – 2007– ص 176.

وفي حالة الإبلاغ أو تقديم شكوى عن نشاط هؤلاء المجرمين لدى السلطات المختصة ممثلة في المصالح الأمنية والقضائية، فإن هذه الأخيرة تباشر أعمال الإستدلال والتحري بشأن الجرائم محل البلاغ أو الشكوى فيبادر ضباط الشرطة القضائية بدءا وقبل كل شيء بالتأكد من الفرضيات التالية في إطار أداء مهامهم:

الفقرة الأولى : الإجراءات الأولية لكشف حقيقة الجريمة.

قبل مباشرة إي إجراء و إتقاءا لتضييع الجهد بشأن جريمة لم تقع ، أو كانت محل تبليغ كاذب ، يباشر ضباط الشرطة القضائيةإلى التاكد من :

أولا : التأكد وقوع جريمة فعلية: فلا بد من أجل ضمان صحة الإجراءات الخاصة أن نكون أصلا بصدد جريمة إلكترونية سواء تحت وصف جنحة أو جناية أي استيفاء الركن الشرعي.[1]

ثانيا : توفر دلائل تشير إلى إتهام شخص معين: ينبغي أن تتوفر في الشخص المشبه فيه دلائل كافية تدعوا للإعتقاد بأنه ساهم في ارتكاب الجريمة مما يستوجب إتهامه فيها، وفي مجال الجرائم المعلوماتية يمكن القول بأن تعبير الدلائل الكافية يقصد به مجموعة من المظاهر والصفات التي تقوم على المضمون المنطقي لملابسات الجريمة وخبرة المحقق.

ثالثا : توفر دلائل كافية وقرائن قوية على حيازة المشتبه فيه لأشياء تفيد في كشف الحقيقة: فلا يكفي لمباشرة تحريات جدية، الحصول على الإذن القانوني فقط، بل يجب أن تتوفر لدى المحقق أسباب كافية بأنه يوجد في مكان ما أو لدى المشتبه فيه أدوات استخدمت في الجريمة المعلوماتية أو أدلة إلكترونية لها فائدة في إستجلاء الحقيقة.[2]

---

[1] – راجع المواد من394 مكرر إلى 394 مكرر 07 قانون العقوبات الجزائري.

[2] – نزيهة مكاري– مرجع سابق– ص 64.

في حال توفر هذه الشروط جاز لأعضاء فريق التحقيق المعلوماتي مباشرة أعمالهم بشأن الجريمة المعلوماتية من خلال تحديد ملابساتها و هوية مرتكبها من خلال إجراءات تسبق عملية الإنتقال لأجل المعاينة المادية لمسرح الجريمة لسبب وحيد و هو أن غالبية الجرائم المعلوماتية هي جرائم غير ملتبس بها، أي أن أعمال البحث و التحقيق بشأنها عادة ما تنطلق متأخرة بعد وقوعها فهي جرائم خفية تحتاج الى خبرات فنية هائلة للكشف عنها و يتبع فريق التحقيق مجموعة من الإجراءات العملية الخاصة نوضحها في الفقرة الموالية.

الفقرة الثانية:إجراء الإرشاد الجنائي .

يعد الإرشاد الجنائي من أهم المصادر التي يعتمد عليها ضباط الشرطة القضائية في عمليات البحث و التحري لجمع المعلومات و خصوصا في مجال الجرائم المعلوماتية فنجد أن هيئات الضبطية أصبحت تجند عناصرها للدخول إلى العالم الافتراضي و بالخصوص إلى مواقع التواصل الإجتماعي و قاعات الدردشة خصوصا تلك المعروف عنها تطرفها و ميول العدوانية، و ذلك تحت أسماء مستعارة يقصد البحث عن الجرائم و مرتكبيها، فضباط الشرطة القضائية ما عليهم سوى الإتصال بالشبكة و اعتماد أسلوب النقاش و الدردشة الإلكترونية مع الغير و مختلف الهيئات و بمجرد بروز مؤشرات عن هوية المجرم المعلوماتي أو جرائم المعلوماتية كالاحتيال أو الإستغلال الجنسي للأطفال ،يبادر هؤلاء إلى سؤاله مثلا عن طرق الحصول على بطاقات الإئتمان المزورة أو عن مواعيد استدراج الأطفال و هي المعلومات التي يستعين بتا مزود الخدمة بالإنترنت الذي يمكن أن يوفر بواسطة برمجيات خاصة مكان وجود المجرم و مثال ذلك ما قامت نه المباحث الفيدرالية الأمريكية **FBI** التي استطاعت الإطاحة بشبكة (FAST–LAND) التي تمتهن القرصنة المعلوماتية و المتاجرة بتا عبر شبكة الأنترنت، و ذلك من خلال دس مرشد معلوماتي ضمن أعضاء هذه الشبكة.[1]

[1] –نبيلة هبة هروال – مرجع سابق – ص 196–197.

و قد أتاح التشريع الجزائري اللجوء إلى هذا الأسلوب حسب ما نصت عليه المادة 65 مكرر 05 ق 06-22 إلى غاية المادة 65 مكرر 18 من قانون الإجراءات الجزائية، و ذلك في حالة الجرائم المعلوماتية، بعد الحصول على إذن مسبب من وكيل الجمهورية أو قاضي التحقيق و تحت رقابة الأول لمدة 04 أشهر قابلة للتجديد.

الفقرة الثالثة: إجراء الوضع تحت المراقبة الإلكترونية.

يجب الإشارة أولا أن المراقبة على أي وسيلة من وسائل الاتصالات تعد بمثابة اعتداء على حرمة الحياة الخاصة فهو حق محمي دستورا[1]، ومشمول بالحماية القانونية التي تقر بأن الاتصالات مهما كان شكلها مكفولة سرا و لا يجوز مصادرتها أو الاطلاع عليها إلا بأمر قضائي مسبب، ويعد فعل مراقبتها أو تسجيلها أو بثها جريمة معاقب عليها، و المراقبة الإلكترونية هي عملية يقوم فيها المراقب بتتبع المشتبه فيه بواسطة الأجهزة الإلكترونية، و إفراغ ما تسفر عنه في تقارير أمنية، وتلك التقارير تفرغ في ملف إلكتروني يحدد فيه الزمان و المكان الذي تمت فيه و النتيجة التي أسفرت عنها.[2]

والحقيقة أن المشتبه فيه المراقب من قبل فريق التحقيق هو شبكة الانترنت أو البريد الالكتروني، إذ يتم من خلالها مراقبة اتصالاته الالكترونية المشتبه فيها، و التقنية المستخدمة في هذا المجال هي التقنية الالكترونية البحتة، و التي تعني مجموعة الأجهزة المتكاملة مع بعضها بغرض تشيكل مجموعة من السمات المتعلقة بالمجرمين أو المشتبه فيهم ،وفق برنامج موضوع مسبقا لتحديدهم من أجل ضبطهم وجمع الأدلة قبلهم لإثبات إدانتهم وتقديمهم أمام المحكمة[3].

---

[1]- تنص المادة 39 من دستور الجمهورية الديمقراطية الشعبية لسنة 1996 على أنه : " لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون ، سرّية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة".

[2]- نابر نبيل عمر- مرجع سابق- ص 149

[3]- نبيلة هبة هروال- مرجع سابق- ص 199-200.

و قد نص التشريع الإجرائي الجنائي الجزائري على إمكانية الوضع تحت المراقبة الالكترونية في مجال مكافحة الجرائم المعلوماتية[1] حسب نصوص المواد 65 مكرر 5 إلى مكرر 10 قانون 06-22 ، وذلك تحت الفصل الرابع الموسوم باعتراض المراسلات و تسجيل الأصوات والتقاط الصور، بحيث يجوز لوكيل الجمهورية و كذلك لقاضي التحقيق في حال فتح تحقيق قضائي ، منح إذن لضابط الشرطة القضائية المكلفين بالبحث و التحري عن الجرائم المعلوماتية، يتضمن اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية دون موافقة المعنيين بها، ويشترط في الإذن أن يكون مكتوبا ومتضمنا لكافة العناصر الأساسية التي تسمح بالتعرف على الاتصالات المطلوب التقاطها وذلك لمدة أقصاها 04 أشهر قابلة للتجديد، ولصاحب الإذن الحق في تسخير أي عون عمومي أو خاص لدى هيئة الاتصالات السلكية أو اللاسلكية من أجل التكفل بالجوانب التقنية المتعلقة بالعملية، وتختتم العملية بإعداد محضر من قبل ضابط الشرطة القضائية يتضمن مضمون العملية مع توضيح تاريخ وساعة بداية العملية و انتهائها، و قد تعزز اللجوء إلى هذا الأسلوب سنة 2009 بموجب نص كل من المادتين 03 و 04 الواردتين ضمن فصول القانون 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها اللتان عبرتا صراحة عن إجازة مباشرة إجراء الرقابة الإلكترونية فيما تعلق بالجرائم المعلوماتية ، و لكن دون ذكر الهيئة المكلفة بتولي ذلك و قد إستمر الوضع كذلك إلى غاية صدور المرسوم الرئاسي 15-261 الذي يحدد تشكلية و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال بتاريخ 08 أكتوبر 2015،

[1]- تنص (المادة 16 مكرر من قانون الإجراءات الجزائية) على المراقبة المادية وليس الإلكترونية.

هذه الأخيرة أصبحت الهيئة المختصة بتنفيذ عمليات المراقبة الإلكترونية للإتصالات الإلكترونية[1] حسب مضمون الفقرة 05 من نص المادة 04 من المرسوم الرئاسي 15-261، و ذلك من خلال إستحداث مديرية المراقبة الوقائية و اليقظة الإلكترونية التي يدخل في صميم إختصاصاتها القيام بمهام المراقبة الإلكترونية للإتصالات من أجل الكشف عن الجرائم المعلوماتية بناء على رخصة مكتوبة من السلطة القضائية و تحت مراقبتها ، حسب ما تقره المادة 11 من المرسوم الرئاسي 15-261، كما منحها القانون حسب نص المادة 21 من المرسوم السالف الذكر الصفة الحصرية لتولي مهام المراقبة الإلكترونية في حال تصنيف الجريمة المعلوماتية ضمن الجرائم الإرهابية و التخريبية و الماسة بأمن الدولة دون سواها من الهيئات الوطنية الأخرى و ذلك تحت سلطة قاض مختص .

وتنفذ عادة عملية المراقبة و التتبع الإلكتروني في مجال الجرائم المعلوماتية من خلال الاستعانة ببعض الوسائل التقنية نذكر منها:

أولا: تقنية تتبع عنوان TCP-IP : عنوان IP هو العنصر المسؤول عن تراسل الحزم البيانية عبر شبكة الانترنت وتوجيهها إلى أهدافها، ويعتبر بمثابة عنوان الحاسوب المتصل بالشبكة ويتكون من شفرة رقمية تتكون من أربع 04 أجزاء، يشر الأول إلى المنطقة الجغرافية و الثاني لرمز مقدم الخدمة، و الثالث لمجموعة الحواسيب المرتبطة و الرابع يخص الحاسوب الذي يتم الاتصال منه، ولذلك وفي حالة وجود جريمة معلوماتية فإن ضباط الشرطة القضائية ضمن فريق التحقيق يقومون بتتبع عنوان IP للجهاز مصدر الجريمة وتحديد موقعه[2].

---

[1] – يقصد بالاتصالات الإلكترونية كل تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها عن طريق أي وسيلة إلكترونية بما في ذلك وسائل الهاتف الثابت و النقال (المادة 05 فقرة 01) من المرسوم الرئاسي 15-261 الذي يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها.

[2] – عبد الله بن سعود بن محمد السراني- مرجع سابق- ص 51.

ثانيا: استخدام تقنية فحص البروكسي (PROXY) : البروكسي هو الوسيط العامل بين الشبكة و المستخدم، تستخدمه الشركات المقدمة لخدمة الاتصال لأجل إدارة الشبكة، وضمان أمنها وتوفير حزمة الذاكرة الجاهزة (Cashe Memory)، يعمل البروكسي على تلقي طلب المستخدم للبحث عن صفحة ما فيتحقق البروكسي ضمن الذاكرة الجاهزة عما إذا جرى تنزيل الطلب من قبل فيقوم بإعادة إرسالها للمستخدم دون الحاجة إلى طلبها من الشبكة العالمية للمعلومات (web) من أجل تزويد المستخدم بها، ومن مزاياه أن ذاكرته هذه يمكن أن تحتفظ بتلك المعلومات و العمليات، وهو ما يمنح لضباط الشرطة القضائية فحصها واستخلاص الدلائل ضد المتهم وذلك من خلال تقفي أثاره بمساعدة مزود الخدمات[1].

ثالثا: استعمال برامج التتبع المعلوماتية: تقوم برامج التتبع على شاكلة برنامج (HACK–TRACER) بالتعرف على محاولات الاختراق ومن قام بها، وإشعار الجهة المتضررة بذلك، وهذه البرامج عادة ما تكون ساكنة في خلفية المكتب، عندما ترصد أي محاولة للقرصنة أو الاختراق وتسارع بغلق منافذ الدخول للمخترق، ثم تبدأ بعملية مطاردته واقتفاء أثره وصولا إلى تحديد عنوانه الإلكتروني (IP) واسم الشركة المزودة بخدمة الانترنت ومعلومات أخرى[2].

رابعا: الاستعانة بنظام كشف الاختراق (INTRUSION DETECTION SYSTEM): وهو النظام الذي يرمز له ب I.D.S وهو نظام يعتمد على مجموعة من البرامج التي تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسوب أو الشبكة مع تحليلها بحثا عن أي إشارة قد تدل على وجود مشكلة تهدد أمن الحاسوب و الشبكة من خلال مقارنة نتائج التحليل مع الصفات المشتركة للاعتداءات

---

[1]- علي عدنان الفيل- مرجع سابق- ص 70-71.

[2]- خالد عياد الحلبي- مرجع سابق- ص 207.

المعلوماتية، ففي حال استئناف أب منها يبادر لتسجيلها في سجلات حاسوبية خاصة (registre) وهي السجلات التي يسعى لها ضباط الشرطة القضائية لتحليل أسلوب ارتكاب الجريمة وربما مصدرها[1].

خامسا: العمل بنظام جرة العسل: هو نظام حاسوبي مخصص لكي يتعرض للهجمات الإلكترونية عبر الشبكة، من خلال خداع من يقوم بذلك وذلك بإبداء سهولة في الاعتداء عليه وذلك لإغرائه، وذلك حتى يتمكن من جمع أكبر قدر من المعلومات عن أسلوب الهجوم وتحليله وهو ما يسمح باتخاذ الإجراءات الوقائية التي تزود فريق التحقيق بالمعطيات اللازمة التي توضح معالم الجريمة[2].

سادسا: جمع الأدلة من خلال اعتراض رسائل البريد الالكتروني: وذلك من خلال الاستعانة ببرامج مصممة للبحث في مضمون الرسائل الالكترونية المتبادلة على شاكلة برنامج كارنيفور و DCS 1000 الذي طورته المباحث الفيدرالية الأمريكية (FBI) الذي يتعقب ويفحص رسائل البريد الالكتروني المرسلة و الواردة عبر أي حاسوب خادم تستخدمه أي شركة توفر خدمة الانترنت وهو برنامج مستخدم في التحقيق في قضايا الأمن القومي الأمريكي[3].

كل هذه الأساليب و البرامج و الأنظمة هي وسائل تساعد ضباط الشرطة القضائية في أعمال البحث و التحري ولكن يبقى أمر استخلاص نتائجها أمرا مرهونا بمدى التزام مقدم خدمة الانترنت بمد يد العون لأجل تحديد مكان ارتكاب الجريمة وهوية مرتكبها.

---

[1]- علي عدنان الفيل- مرجع سابق- ص 71-72.

[2]- خالد عياد الحلبي- مرجع سابق- ص 209.

[3]- نبيلة هبة هروال- مرجع سابق- ص 201.

الفقرة الرابعة: التزامات مقدمي خدمات الانترنت في مجال مساعدة أعمال البحث و التحري.

يقصد بمزود الخدمات أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات لأجل التواصل بواسطة تقنية المعلوماتية، ويقوم بتخزين ومعالجة المعطيات بما فيها المعلومات الخاصة بالمشترك كنوع خدمة الاتصالات المستخدمة لديه، هويته، عنوانه البريدي، رقم هاتفه وذلك بناء على اتفاق ترتيب الخدمة القائم بينهما، حسب تعريف المادة 02 الفقرة 02 و 09 من الاتفاقية العربية لمكافحة الجرائم المتصلة بالتقنية المعلوماتية

كما يعرفه قانون حماية الحياة الخاصة في مجال الاتصالات الالكترونية الأمريكية (ECDA) بأنه نوعان:

- الأول مزودو خدمة الاتصالات الالكترونية وهو كل من يقدم خدمة إلى مستخدمي الشبكة، ويعمل على تسهيل إرسال واستقبال الاتصالات السلكية و اللاسلكية و الالكترونية.
- الثاني مزودو خدمة معالجة المعلومات عن بعد ، وهو كل من يقدم للجمهور خدمة معالجة البيانات عن بعد بواسطة وسائل الاتصالات الالكترونية.

وبناء على ذلك فإذا أرسل أي شخص لآخر رسالة عن طريق البريد الإلكتروني فإنها تمر و بالضرورة على مزود الخدمة وتخزن لديه[1].

إن القانون قد سمح للسلطات المختصة بمتابعة الجرائم المعلوماتية حق طلب التحفظ على البيانات المخزنة لديها وحق كذلك تزويدها بالمعلومات الخاصة بالمشترك ونشاطه في إطار عملها المتعلق بأعمال البحث و التحري عن الجرائم المعلوماتية.

[1]- عائشة بن قارة- مرجع سابق- ص 155-156.

وهو الإجراء و الالتزام الذي نجد له أصلا قانونيا على المستوى الدولي حسب ما تقرره أحكام المادتين 16 و 17 من اتفاقية بودابست لمكافحة الجرائم المعلوماتية، تقابلها المواد 23-24-25 من الاتفاقية العربية لمكافحة الجرائم المتصلة بالتقنية المعلوماتية، وقد وردت هذه الالتزامات على المستوى الوطني حسب ما جاء في نص المادة 10 من الفصل 04 من قانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ، التي توجب على مقدمي خدمة الانترنت مساعدة السلطات في إطار التحريات القضائية من خلال جمع و تسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، وبوضع المعطيات التي يتعين عليهم حفظها تحت تصرف السلطات المذكورة وكل ذلك تحت غطاء السرية ، كما ألزمت المادة 11 من نفس القانون مقدمي الخدمات حفظ المعطيات التالية:

- المعطيات التي تسمح بالتعرف على مستخدمي الخدمة.
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة.
- المعطيات التي تسمح بالتعرف على المرسل إليه وعناوين المواقع المطلع عليها.

ويلزم حفظ هذه المعطيات لمدة سنة منذ تاريخ تسجيلها، وهي مدة طويلة مقارنة بمقترحات الاتفاقية العربية التي قدرتها ب 90 يوما أو بما يحدده الاتحاد الأوروبي وفق الأمر 95/46 EC بالمدة الضرورية ، وهو الأجل الذي يسمح لضباط الشرطة القضائية بالرجوع إليها من أجل تحديد هوية وأماكن ارتكاب الجرائم المعلوماتية وذلك نظرا للاعتبارات التالية:

- قابلية البيانات المعلوماتية للتلاشي و التلاعب و التغير.
- ارتكاب غالبية الجرائم عن طريق نظم الاتصالات وهو ما يساعد على تحديد هوية مرتكبي هذه الجرائم.

- التحفظ على هذه البيانات يعتبر أحد أهم عناصر الإثبات التي يمكن أن تكشف عن هوية مرتكبي هذه الجرائم[1].

ولضباط الشرطة القضائية إمكانية تقديم طلبات لمزودي الخدمة بالانترنت لأجل تزويدهم بالمعلومات المخزنة و من ضمن هذه الطلبات:

- طلب التحفظ المعجل على البيانات المخزنة وذلك حتى يتفادى المزود شطب التسجيلات و القضاء على الدليل.
- طلب تقديم بيانات معلوماتية خاصة بالمشترك.
- طلب اعتراض الاتصالات الالكترونية.

إذن تعتبر هذه الإجراءات أهم الإجراءات ذات الطابع الإجرائي الفني و المعلوماتي في مجال أعمال البحث و التحري عن الجرائم المعلوماتية التي يباشرها ضباط الشرطة القضائية تنفيذا لتعليمات وكيل الجمهورية أو قاضي التحقيق أو اختصاصا منهم، وذلك من خلال ممارسة مهامهم بعيدا عن مسرح الجريمة أي في مرحلة تسبق التنقل للمعاينة و التفتيش المادي وضبط الأدلة الالكترونية و المادية وهي الإجراءات التي تختلف نوعا ما من حيث الوسائل و الطرق وهي التي ستكون محل بحثنا في المطلب الموالي.

---

[1]- هلالي عبد اللاه أحمد- مرجع سابق- ص 197-198.

المطلب الثالث: الإجراءات الفنية الخاصة بمعاينة مسرح الجريمة المعلوماتية.

بعد أن تطرقنا إلى المسائل الخاصة بإجراءات البحث و التحري الأولية بشأن الجريمة المعلوماتية و التي يبادر إليها ضباط الشرطة القضائية، بمجرد الوصول إلى علمهم بوقوع الجريمة، تنتقل إلى تفصيل المسائل الخاصة بالإجراءات العملية ذات الطابع الخاص المتعلقة بمرحلة المعاينة و التفتيش و التي يتم عادة على مسرح الجريمة، و التي تقتضي تنقل الجهات المختصة من أجل تحقيق الهدف الرئيسي وهو إحراز الأدلة المادية والإلكترونية، و التي من شأنها إثبات وإدانة أو براءة المتهم، وعادة ما يتولى مهمة التنقل إلى مسرح الجريمة المعلوماتية، الفرقة الخاصة بالبحث و التحقيق في مسائل الجرائم المعلوماتية، نظرا لتوفرهم على معارف تسمح لهم بالتعامل الصحيح مع أدلتها، و لا يتم الانتقال إلى مسرح الجريمة إلا لفرضيتين اثنتين:

- فرضية مداهمة مسرح الجريمة المتلبس بها، وهو أمر مستبعد جدا إذا لم نقل نادرا، نظرا لخصوصية الجريمة و المجرم المعلوماتي، اللذان يتميزان بالخفاء و السرية في تنفيذ الجريمة إضافة إلى صعوبة كشفها.
- فرضية تنفيذ المهام الموكلة لهم إما من تلقاء أنفسهم بناء على بلاغ أو شكوى بشأن جريمة معلوماتية، أو تنفيذا لأوامر وكيل الجمهورية أو قاضي التحقيق، وهي الفرضية الأقرب للتجسيد نظرا إلى ضرورة تضافر الجهود الفنية و القانونية لأجل مكافحة الجرائم المعلوماتية.

وعليه فإننا سنحاول أن نضع في هذا المطلب تصورا قانونيا تقنيا وفنيا لجملة الإجراءات الواجب إتباعها عند الانتقال إلى مسرح الجريمة المعلوماتية، بغرض ضبط الأدلة الإلكترونية وذلك حسب تسلسل الفروع التالية:

- الفرع الأول: الإجراءات الخاصة بالانتقال إلى مسرح الجريمة وتأمينه.

- الفرع الثاني: الإجراءات الخاصة بالتفتيش وضبط الأدلة الإلكترونية.
- الفرع الثالث: الأساليب الخاصة في التعامل مع الأشخاص ذوي العلاقة بالجريمة المعلوماتية.

الفرع الأول: الإجراءات الخاصة بالانتقال إلى مسرح الجريمة وتأمينه.

إذا ثبت بناء على أعمال البحث و التحري الأولية التي قام بها ضباط الشرطة القضائية بشأن صحة فحوى البلاغات الواردة إليهم بشأن وقوع جريمة معلوماتية أو بناء على توفر حالة تلبس بالجريمة، أنه هناك أدلة قوية تشير إلى حيازة المشتبه فيه لأدلة تفيد في استجلاء الحقيقة، مخزنة على حاسوبه أو على وسائط خارجية أو مخبأة في مسكنه أو مقر عمله فإن هذا الأمر يستدعي و بالضرورة الانتقال إلى مسرح الجريمة المفترض لأجل إتمام أعمال البحث و التحري أو القيام بتنفيذ الأوامر القضائية الواردة من قاضي التحقيق كالأمر بالتفتيش، وإن كانت الإجراءات الخاصة بالانتقال إلى مسرح الجريمة المعلوماتية نوعية بعض الشيء إلا أنها تخضع و بالضرورة لمجموعة من الشروط القانونية قبل كل شيء.

الفقرة الأولى:ضرورة إستيفاء الشروط القانونية لتنفيذ أمر الانتقال.

إن الانتقال إلى مسرح الجريمة وما يصاحبه من ضرورة المعاينة و التفتيش، يقتضي التعدي على حرمة الحياة الشخصية للأفراد ومساكنهم، يستوجب أن يتم في إطار قانوني لأجل ضمان شرعية الإجراءات وعدم تعريضها للبطلان الذي قد يهدم الدليل ويتسبب في إفلات المتهم من العدالة، إضافة إلى ضمان عدم التعسف في مواجهة الغير من الأفراد بحجة ضرورة التحقيق، وتجنبا لكل ذلك يستوجب القانون على ضابط الشرطة القضائية احترام مجموعة من الشروط القانونية المبنية في قانون الإجراءات الجزائية وأخرى في القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ، لأجل إتمام هذه الإجراءات ضمن إطار شرعي وذلك حسب الأحوال التالية:

أولا– حسب أحوال حالة التلبس : توصف الجناية أو الجنحة بأنها في حالة تلبس إذا كانت مرتكبة في الحال أو عقب ارتكابها، كما تعتبر كذلك إذا كان الشخص المشتبه فيه في وقت قريب جدا من وقوعها أو تبعته العامة بالصياح أو كان حائزا لأشياء أو دلائل تدعوا إلى افتراض مساهمته في الجريمة، كما توصف كذلك إذا ما ارتكبت الجناية أو الجنحة في منزل أو كشف صاحب المنزل عنها عقب وقوعها وبادر باستدعاء ضابط الشرطة القضائية لأجل إثباتها[1].

إن تطبيق هذه الأحوال على الجريمة المعلوماتية يكاد أن يكون أمرا مستحيلا، غير أنه يمكن افتراض وقوعها ولو في نادر الأحوال وهو ما يترتب عنه اتخاذ الإجراءات التالية:

- على ضابط الشرطة القضائية الذي بلغ بجناية أو جنحة متلبس بها مهما كان نوعها، أن يخطر وعلى الفور وكيل الجمهورية، ثم ينتقل وبدون تمهل إلى مسرحها قصد اتخاذ الإجراءات اللازمة للتحري، و التي تسمح بالحفاظ على الآثار التي يخشى اختفائها.[2]
- لا يجوز الانتقال إلى مسكن الأشخاص الذين يظهر أنهم ساهموا في الجريمة المتلبس بها، سواء لتنفيذ إجراءات التحري أو التحقيق بالجرائم المعلوماتية إلا بناء على إذن مكتوب من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهاره قبل الدخول إلى مسكن المشتبه فيه، ويترتب على تنفيذ الإجراء في غياب الإذن ،أو غياب أوصاف محل البحث ، أو عناوين أماكن البحث ، عن مضمون الإذن البطلان المطلق للإجراء برمته[3]

---

[1]– المادة: 41 قانون الإجراءات الجزائية الجزائري.

[2]– المادة: 42 قانون الإجراءات الجزائية الجزائري.

[3]– المادة 44 ق 06–22 قانون الإجراءات الجزائية الجزائري.

فبمجرد توفر هذين الشرطين جاز لرجال البحث و التحقيق بناء على حالة التلبس مباشرة أعمالهم المتعلقة بالمعاينة و التفتيش، ولهم الحق في إتمام أعمالهم في أي ساعة من ساعات الليل أو النهار وذلك حسب ما تورده المادة 47 من قانون الإجراءات الجزائية.

ثانيا- حسب ظروف الأحوال العادية : يقصد بها الحالات التي تكون خارج حالة التلبس وهي الظروف التي تميز الجريمة المعلوماتية ، و التي تحتاج إلى تقدير فني كبير لأجل التأكد من مدى صحة وقوعها، واتخاذ تقرير الإجراءات الكفيلة بمتابعة مرتكبيها واثبات الأدلة في مواجهتهم، ويتم الانتقال إلى مسرح الجريمة تنفيذا عادة لأوامر وكيل الجمهورية في إطار إتمام إجراءات البحث و التحري[1]، أو تنفيذا لأوامر قاضي التحقيق[2].

ويشترط في هذه الحالة احترام جملة الشروط المتعلقة بالإذن المكتوب سواء الصادر من قبل وكيل الجمهورية و قاضي التحقيق حسب الأحكام الواردة في المواد من 44 إلى 47 مكرر من قانون الإجراءات الجزائية تحت طائلة البطلان.

إذن فمن الناحية القانونية فإن الشروط المتعلقة بالمعاينة و التفتيش في إطار الجريمة المعلوماتية هي نفس الشروط المتبعة في باقي الجرائم الأخرى و لا داعي لتكرارها، بحيث ينبغي تركيز البحث حول طبيعة الإجراءات المتبعة و الاحتياطات الخاصة التي يطبقها ضباط الشرطة القضائية لأجل معاينة الجرائم المعلوماتية و التي تعرف تحت اسم إجراءات تأمين موقع الجريمة المعلوماتية.

---

[1]- المادة 36 فقرة 04- المعدلة بموجب الأمر 15-02 قانون الإجراءات الجزائية الجزائري.

[2]- المادة 68 ق – 01-08- قانون الإجراءات الجزائية الجزائري.

الفقرة الثانية: الإلتزام بإجراءات تأمين موقع الجريمة المعلوماتية.

قد يقوم كل من ضباط الشرطة القضائية أو وكيل الجمهورية أو قاضي التحقيق ، عند الانتقال إلى مسرح الجريمة بأعمال المعاينة المادية و الميدانية للجريمة في حد ذاتها، و المعاينة هي فحص مكان أو شيء أو شخص له علاقة بالجريمة، و إثبات حالته كمعاينة مكان ارتكاب الجريمة أو أداة ارتكابهما أو محلها أو معاينة جسم أو ملابس الجاني أو المجني عليه لإثبات ما بالجسم من جراح أو ما على الثياب من دماء أو آثار أخرى[1].

إن الإنتقال من أجل إجراء المعاينة يعتبر أول إجراء من إجراءات البحث و التحري ، فهو الإجراء الأكثر أهمية لآنه يسمح بالمعاينة المادية للوقائع المشكلة للجريمة ، و الإنطلاق بشكل سريع و مباشر في عملية البحث و ضبط الأدلة ، التي تساعد على معرفة وقت و كيفية إرتكاب الجريمة و هوية فاعلها، و عادة ما تسند هذه المهمة لأفراد الشرطة العلمية و التقنية ، نظرا لضرورة التدخل بسرعة و بطريقة مدروسة تتلائم و طبيعة الجريمة محل المعاينة ، من خلال القيام بسلسلة من العمليات التي تستلزم خبرة ميدانية و وسائل من نوع خاص.[2]

غير أن دورها يتضاءل في مجال الجرائم المعلوماتية، فهي لا تحقق نفس الأهداف كما هو الحال في الجرائم التقليدية، كما أنها لا ترقى إلى درجة أهميتها كإجراء في تلك الجرائم وذلك راجع إلى :

1. أن الجرائم التي تقع على نظم المعلومات و الشبكات قلما تخلف عقب ارتكابها أثار مادية.

---

[1]- عبد العال الدريبي- مرجع سابق- ص 294.

[2] -Charle Diaz – La Police Techenique et Scientifique-2eme Edition- Edition Presse universitaire de France - France – 2006- p54.

2. إن عددا كبيرا من الأشخاص قد يتردد على مسرح الجريمة خلال الفترة الزمنية التي تتوسط مرحلة ارتكابها واكتشافها، مما يفسح المجال أمام حدوث تلف أو تغيير أو عبث بالآثار المترتبة عنها[1].

وحتى تكون للمعاينة في جرائم المعلوماتية فائدة تسهم في كشف الحقائق وجب على المحقق اتباع مجموعة الإرشادات العملية ذات الطابع التأميني نوجزها فيما يلي:

أولا- قبل التنقل إلى إجراء المعاينة: يجب إتباع الخطوات التالية من قبل رجال البحث و التحقيق قبل التحرك إلى مسرح الجريمة المعلوماتية لإجراء المعاينة وهي:

1. توفير معلومات مسبقة عن مكان الجريمة، وكذلك عن نوع وعدد الأجهزة المتوقع مداهمتها، ونوع الشبكات المتصلة بها، وذلك لتحديد خطة التعامل معها.
2. إعداد خريطة الموقع الذي سيتم الانتقال إليه مع ضرورة وضع خطة وتقسيم الأدوار على فريق التحقيق وتحديد المهام واختصاص كل واحد منهم حتى لا تتداخل الاختصاصات.
3. الحصول على الاحتياجات الضرورية من الأجهزة و البرامج الحاسوبية للاستعانة بها في الفحص.
4. تأمين مصدر التيار الكهربائي حتى لا يتم التلاعب به عن طريق قطعه أو تعديله بهدف تعطيل عمل فريق المعاينة.
5. مراجعة الخطة واستحضار الإذن القضائي.[2]
6. **ثانيا: عند معاينة مسرح الجريمة:**المعاينة إجراء من أهم إجراءات التحقيق الجنائي لأهمية الأدلة المستقاة منها التي تكون غالبا ذات دلالة قاطعة في الإثبات ، و قد أكدت المعاينة الفنية في كثير من الأحيان فعاليتها في إظهار حقيقة الجريمة و معرفة كيفية و أسباب وقوعها و هوية مرتكبيها ، لذلك يترتب على

---

[1]- علي عدنان الفيل- مرجع سابق- ص 33.

[2] – نبيلة هبة هروال – مرجع سابق – ص 220.

المحقق مراعاة الدقة و الترتيب و بذل أقصى ما يمكن من العناية و الإهتمام عندإجرائها ، للحيلولة دون فقدان ما يمكن إستخلاصه من معلومات قيمة قد تفيد في تنوير التحقيق ، و يرى الفقه الجنائي ضرورة إتباع ضوابط خاصة لأجل معاينة مسرح الجريمة المعلوماتية هي[1]:

1–تحديد أجهزة الحواسيب الموجودة وتحديد مواقعها بأسرع وقت ممكن، إضافة إلى البحث عن النهاية الطرفية المزود للخدمة بالانترنت (MODEME) من أجل قطع الاتصالات الخارجية التي يمكن أن تخرب الأدلة أو تمحوها من على ذاكرة الحاسوب، كما يراعى ضرورة تصوير الأجهزة الموجودة وخاصة الأجزاء الخلفية التي تحمل الأرقام التعريفية للأجهزة.

2–ضرورة وضع حراسة كافية على مكان المعاينة ومراقبة التحركات داخل مسرح الجريمة، مع رصد الاتصالات الهاتفية من و إلى مسرح الجريمة مع إبطال مفعول الهواتف النقالة التي تساعد عن طريق تقنية الجيل الثالث في تدمير الأدلة من خلال اتصالها بالأجهزة محل المعاينة[2].

3–ملاحظة وإثبات الطريقة التي تم بها إعداد النظام و الآثار الإلكترونية وبوجه خاص السجلات الإلكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع الاتصال وطريقة الولوج للنظام إضافة إلى ملاحظة و إثبات حالة التوصيلات و الكابلات المتصلة بالنظام حتى يمنح فرصة لإجراء المقارنة حين يعرض الأمر على القضاء[3].

---

[1]–عبد الفتاح عبد اللطيف الجبارة – إجراءات المعاينة الفنية لمسرح الجريمة–الطبعة الأولى– دار الحامد للنشر و التوزيع– عمان– الأردن – 2010– ص 171.

[2]عبد الفتاح بيومي حجازي– الجوانب الإجرائية لأعمال البحث والتحقيق الإبتدائي في الجرائم المعلوماتية– دراسة مقارنة على ضوء القواعد العامة للإجراءات الجنائية – مرجع سابق– ص 587.

[3]– عبد الله حسن علي محمود– مرجع سابق – ص 02.

4-عدم التسرع في نقل أي "مادة معلوماتية" من مسرح الجريمة وذلك قبل إجراء اختبار اليقين من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي و التي قد تؤدي إلى إتلاف البيانات المخزنة مباشرة في حالة تعرضها لها.

5-حفظ ما تحتويه سلة المهملات من أوراق ممزقة أو كربون نسخ أو أقراص ممغنطة سليمة أو محطمة مع فحصها ورفع البصمات عنها وكذلك التحفظ على مستندات الإدخال و المخرجات الورقية و التي عادة ما تكون ذات صلة بالجريمة[1].

6-حصر عملية المعاينة في فئة المختصين و المحققين الذين يتوافرون على الكفاءة العلمية و الخبرة الفنية في مجال النظم المعلوماتية، و الذين تلقوا تدريبا فنيا كافيا على التعامل مع الأدلة المعلوماتية، ففي فرنسا مثلا يقوم فريق التحقيق المتكون من ثلاث عشر (13) شرطيا بالإشراف على تنفيذ المهام التي يأمر بها وكيل الجمهورية أو قاضي التحقيق، فيرافقون المحققين أثناء عمليات المعاينة ويعملون على فحص الأجهزة ونسخ محتوياتها وإعداد تقارير فنية ترسل إلى قاضي التحقيق[2].

إذن تعتبر هذه مجموعة من الإجراءات و التدابير العملية الفنية ذات الطابع الخاص بمسائل المعاينة و التي تجري على مسرح الجرائم المعلوماتية و التي تعتبر ضرورية لأجل إتمام أعمال التفتيش و الضبط اللاحقة.

---

[1]- فتوح الشاذلي- عفيفي كامل عفيفي- مرجع سابق - ص 357.

[2]- علي عدنان الفيل- مرجع سابق- ص 35.

الفرع الثاني: الإجراءات الخاصة بالتفتيش و ضبط الأدلة.

يهدف التفتيش إلى ضبط الأدلة المادية التي تفيد في كشف الحقيقة، و الضبط غاية التفتيش القريبة أي الأثر المباشر الذي يسفر عنه الإجراء، و هدف التفتيش سواء تعلق بالأشخاص أو المساكن هو ضبط الأشياء التي تفيد في كشف الحقيقة أي الأشياء التي تعد في ذاتها دليلا على الجريمة، أو يمكن استخدامها كدليل، وقد تكون هذه الأشياء هي وسيلة الجريمة أو تكون السبب الذي ارتكبت من أجله الجريمة، ولما كان الضبط هو الأثر المباشر للتفتيش، وباعتباره أحد إجراءات التحقيق فتنطبق عليه القواعد التي تنطبق على التفتيش فإذا بطل التفتيش بطل الضبط، و التفتيش يعتبر وسيلة تهدف للوصول إلى الحقيقة وليس غاية في حد ذاته، ولعل أن الشكل الذي يتبادر إلى الذهن في هذه الحالة هو مدى قابلية النظم المعلوماتية للتفتيش باعتبارها بيانات مادية.[1]

لقد سبق وأن فصلنا في الإجابة عن هذا التساؤل في المبحث الأول من الفصل الثاني، ولقد خلصنا في شأن ذلك بأن أغلب التشريعات قد أقرت بالطبيعة الخاصة للمعلومات وجعلت من موضوعها محل قابلا للتفتيش و الضبط شأنها شأن البيانات المادية، وذلك من خلال إقرار النصوص الإجرائية الجزائية بقواعد تنظم عمل جهات التحقيق فيما تعلق بمسألة التفتيش في مجال الجرائم المعلوماتية كما سبق وأن أشرنا إليه ، وبالتالي فإننا سنستعرض بالبحث ضوابط التفتيش و الضبط القانونية و الفنية في مجال الجرائم المعلوماتية.

---

[1]- على حسن محمد الطوالبة- التفتيش الجنائي على نظم الحاسوب و الإنترنت- مرجع سابق- ص 135.

الفقرة الأولى: الضوابط القانونية للتفتيش و الضبط.

إن الحديث عن مسألة الضوابط القانونية للتفتيش و الضبط في مجال الجرائم المعلوماتية يقودنا إلى إبرازها وفق التسلسل المنطقي التالي:

أولا : حسب شروط الاختصاص النوعي و المحلي: على عكس أغلبية التشريعات العربية التي خولت سلطة التحقيق وحق التفتيش للنيابة العامة، فإن التشريع الإجرائي الجزائريساير نظيره الفرنسي وجعل الاختصاص الأصيل بالتفتيش و الضبط لقاضي التحقيق، و لا يحق ذلك للنيابة العامة ممثلة في وكيل الجمهورية إلا وفق حالة التلبس بالجنحة أو الجناية.

فلقاضي التحقيق أن يقوم وفقا للقانون باتخاذ جميع إجراءات التحقيق التي يراها مناسبة وضرورية للكشف عن الحقيقة بالتحري عن أدلة الاهتمام و أدلة النفي ، ويجوز له بناء على ذلك الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، ويباشر قاضي التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقية (المادة79-80- 81)قانون الإجراءات الجزائية الجزائري.

وإذا كان من المتعذر على قاضي التحقيق أن يقوم بنفسه بجميع إجراءات التحقيق جاز له أن ينتدب ضابط الشرطة القضائية للقيام بتنفيذ جميع أعمال التحقيق اللازمة ضمن الشروط القانونية المنصوص عليها في المواد من 138 إلى 142 من قانون الإجراءات الجزائية[1] .

وباعتبار التفتيش و الضبط إجراء يستهدف جرائم عادة ما تقع إما داخل الاختصاص المحلي لقاضي التحقيق أو خارجه، فإن هذا الأخير ملزم بإتباع قواعد الاختصاص الإقليمي فهو مختص ضمن

---

[1]- المادة 68 ق 01- 08 قانون الإجراءات الجزائية الجزائري.

دائرة وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه فيهم، أو بمحل القبض على أحدهم، ويمتد اختصاصه تلقائيا إلى دائرة اختصاص محاكم أخرى فيما يتعلق بالجرائم المعلوماتية فاختصاصه في هذه الحالة وطني حسب ما هو مقرر بالمادة (40 ق 04- 14 ق إ ج) وكذلك الفقرة الأخيرة من نص (المادة 47 ق 06-22 ق إ ج) ، وهو نفس الاختصاص المقرر إقليميا المطبق على ضباط الشرطة القضائية في حال تنفيذ أوامر قاضي التحقيق.[1]

ثانيا: من حيث المواعيد : عندما يتعلق الأمر بالجرائم المعلوماتية فإنه يجوز التفتيش في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل بناء على إذن مسبق من وكيل الجمهورية المختص.

يمكن لقاضي التحقيق أن يقوم بنفسه بعملية التفتيش و الضبط ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يندب ضابط الشرطة القضائية المختص بذلك (الفقرة 03 و 04 المادة 47 ق 06-22) من قانون الإجراءات الجزائية الجزائري.

غير أنه إذا ما تعلق الأمر بجناية فلا يجوز سوى لقاضي التحقيق القيام بالتفتيش وبحضور وكيل الجمهورية (المادة 82 ق إ ج)، و الملاحظ أن هذا الاستثناء هو بمثابة نص مضاد لما هو وارد في نص المادة 47 الفقرة 03 و 04 و التي تمنح الحق لضباط الشرطة القضائية المختصين بالجرائم المعلوماتية بالتفتيش في مسرح الجريمة المعلوماتية، فكان من الأولى توسيع مجال اختصاصهم وليس تضييقه من خلال حصر الاختصاص في شخص قاضي التحقيق الذي قد لا يكون على علم بتقنيات التفتيش الخاصة بالجرائم المعلوماتية.

---

[1]- الفقرة الأخيرة المادة 16 ق 06-22 قانون الإجراءات الجزائية الجزائري.

أما فيما تعلق بمسألة حضور المشتبه فيه عملية التفتيش و الضبط سواء في مسكنه أو مسكن شخص آخر فإن الفقرة الأخيرة من نص (المادة 45 ق 22-06 ق إ ج) لا تستوجب حضوره، ففي مجال الجرائم المعلوماتية لقاضي التحقيق أو لضباط الشرطة القضائية مباشرة أعمالهم دون مراعاة هذه المسألة مع ضرورة الالتزام بأحكام ضمان السر المهني و التقييد بقواعد الحجز.

وإذا ما كان الشخص موقوفا للنظر أو محبوسا مؤقتا أو غائبا لسبب آخر وكان من الخطر نقله لمكان التفتيش فإنه يجوز إجراء التفتيش بعد الحصول على الموافقة المسبقة لوكيل الجمهورية، أو لقاضي التحقيق مع ضرورة حضور شاهدين(المادة 47 مكرر ق 06-22 ق إ ج).

الفقرة الثانية: القواعد الفنية المتبعة عند التفتيش والضبط .

إذا ما استنفذت الشروط القانونية لمباشرة إجراء التفتيش، جاز لقاضي التحقيق أو لضباط الشرطة القضائية المختصين، مباشرة عملية التفتيش و الضبط، بغرض حجز كل ما من شأنه إظهار الحقيقة المتعلقة بالجريمة المعلوماتية سواء أكانت مادية كالحاسوب وملحقاته أو منطقية كالمعلومات و البيانات المخزنة عليه، أو على الشبكة، و لابد أن يرعى في ذلك القواعد التالية:

أولا: القواعد الاحتياطية قبل بدء التفتيش المعلوماتي:

1- السيطرة على المناطق المحيطة بمسرح الجريمة أو مكان وجود النظام المعلوماتي من خلال غلق المداخل و المخارج.

2- السيطرة على الدائرة المحيطة بمسرح الجريمة بوضع حراسة ملائمة.

3- السيطرة على محيط مسرح الجريمة من خلال التحفظ على الأشخاص الموجودين.

4- وضع حراسة على الأجهزة حتى لا يتمكن أي كان من لمسها.

5- اختيار مكان لمقابلة المتهمين و الشهود بعيدا عن الأجهزة.

6- توثيق مسرح الجريمة أو محل التفتيش جيدا من خلال جرد محتوياته وذلك لاحتمال توفر إحدى هذه المصادر على الدليل وهي الأوراق التي تم طباعتها، جهاز الحاسوب وملحقاته، أقراص ودعائم البرامج، وسائط التخزين المتحركة، الطابعات[1].

ثانيا: قواعد تفتيش و ضبط ماديات الجريمة المعلوماتية: يخضع تفتيش المكونات المادية للحاسوب للإجراءات القانونية الخاصة بالتفتيش، أي أنه يجب أن يراعى مكان وجود ذلك الحاسوب أثناء مباشرة الإجراء فيما كان مكانا عاما أو خاصا واستنفاذ الشروط القانونية السالفة الذكر[2].

ويراعى عند التفتيش لأجل ضبط الأدلة المحتملة القواعد التالية:

1. التركيز حول مكان شاشة الحاسوب التي تعتبر الموضع المفضل عند مجرمي المعلوماتية للصق بعض القصاصات التي تحمل المعلومات المهمة كأرقام الهاتف أو فهرس المعلومات داخل الحاسوب كالكلمات السرية و المرور.
2. التفتيش بجوانب التوصيلات الهاتفية، فعادة ما يدون مجرمو المعلوماتية محادثاتهم الهاتفية في شكل مخططات يتركونها بجوار الهاتف.
3. تفتيش المفكرات الالكترونية، وهي من أهم الأدلة التي يجب التحفظ عليها وضبطها فهي تحمل أرقام الهاتف، وعناوين البريد الإلكتروني و المواعيد و الملخصات وغيرها من المعلومات المفيدة في التحقيق.
4. تفتيش جيوب المتهم، فمجرمو المعلوماتية معهم عادة أقراص مرنة، أو بطاقات ذاكرة، تحمل معلومات متعلقة بالجريمة عادة[3].

ويحق لرجال التحقيق الإطلاع على محل التفتيش وحجزه أو ضبطه وتوضع عادة الأشياء المحجوزة في وعاء أو كيس، يغلق ويختم عليها بختم قاضي التحقيق أو ضابط الشرطة القضائية.

---

[1]- علي عدنان الفيل- مرجع سابق- ص 36-37.

[2]- نبيلة هبة هروال- مرجع سابق- ص 237.

[3]- حسن طاهر داود- جرائم نظم المعلومات- الطبعة الأولى- أكاديمية نايف للعلوم الأمنية- الرياض- المملكة العربية السعودية- سنة 2000- ص 228.

ثالثا: قواعد تفتيش وضبط المكونات المنطقية : يجوز للسلطات القضائية المختصة (قاضي التحقيق)، ولضباط الشرطة القضائية حسب ما يجيزه القانون 09-04 المتعلق بمكافحة الجرائم المعلوماتية و في إطار إجراءات التحقيق المعلوماتي، الدخول بغرض التفتيش ولو عن بعد إلى كل منظومة معلوماتية أو جزء منها وإلى كل منظومة تخزين معلوماتية.

وإذا كانت هناك أسباب تدعوا للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى غير تلك الأولى جاز لهم تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا ، وإذا كانت المعطيات المبحوث عنها مخزنة في منظومة معلوماتية خارج الإقليم فإن الحصول على إذن يكون من خلال طلب مساعدة دولية حسب المبادئ و الأعراف الدولية في مجال التعاون القضائي.[1]

وهي آلية التفتيش عن بعد أو التفتيش المباشر التي تستهدف الكيانات المعنوية و المنطقية للحاسوب دون المادية منها، وإن كانت هذه الأخيرة ضرورية لأجل ولوج النظم المعلوماتية أو الشبكات بهدف التفتيش عن بعد و إلى حجز المعطيات المعلوماتية، فعندما تكتشف السلطة المختصة بالتفتيش المعلوماتي وجود معلومات مهمة من شأنها الكشف عن الجريمة ومرتكبها ويقدر بأنه لا حاجة لضبط وحجز ماديات المنظومة المعلوماتية، فإنه يقوم بنسخ المعطيات و المعلومات الضرورية لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز و الوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية، مع السهر على سلامة المعطيات الأصلية المخزنة على المنظومة المعلوماتية محل التفتيش[2].

---

[1]– المادة 05– قانون 09–04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال.

[2]– المادة 06 قانون 09–04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال.

أما إذا استحال أمر حجز هذه المعطيات لأسباب تقنية كان للسلطة المختصة بالتفتيش و الحجز أن تستعمل تقنيات المنع من الوصول إلى المعطيات أو نسخها كما يجوز لها أن تأمر باتخاذ جميع الإجراءات اللازمة لمنع الإطلاع عليها وحجبها من خلال تكليف أي شخص مؤهل وذلك باستعمال وسائل تقنية لذلك[1].

الفقرة الثالثة: وسائل تحليل الأدلة المحجوزة.

إن عملية التفتيش عادة ما تسفر عن نوعين من المضبوطات مادية ومنطقية، فالأولى في شكل الحاسوب ذاته وملحقاته، و الثانية في شكل ملفات وبيانات ومعلومات كانت مخزنة على القرص الصلب للحاسوب أو على الشبكة، وهي المضبوطات التي تحتاج إلى تحليل من أجل استخلاص الدليل منها وذلك من خلال الاستعانة ببرامج ووسائل خاصة نوجزها فيما يلي:

أولا: وسائل استعادة الدليل وفك التشفير : قد يقدم المتهم على تخريب القرص الصلب لحاسوبه بمجرد علمه باكتشاف أمره، ولذلك يستعين أعضاء فرقة البحث و التحقيق المعلوماتي، في مجال معالجة الأدلة التالفة ببرنامج (VIEW DISK)، أما في مجال فك التشفير الذي قد يعمد الجاني إلى استعماله لمنع الإطلاع على البيانات المخزنة على حاسوبه فتستعمل برامج شركة ACCES DATA CORPORATION تحت اسم PASS OUT أو (PASSWORD RECOVERY)[2].

ثانيا: برامج إذن التفتيش : هو برنامج قاعدة بيانات يسمح بإدخال كل المعلومات الهامة المطلوبة، لترقيم الأدلة وتسجيل البيانات عنها، ويقوم هذا البرنامج بإصدار وصلات استلام الأدلة، و البحث في

---

[1]- المادة 07و 08 قانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

[2]- ممدوح عبد الحميد عبد المطلب- مرجع سابق- 84-85.

قوائم الأدلة المضبوطة لتحديد مكان دليل معين أو ظروف ضبط هذا الدليل، وعادة ما يكون بحوزة المحقق على قرص مرن أو قرص صلب محمول.

ثالثا: برنامج بدء تشغيل الحاسوب: وجود قرص بدء تشغيل الحاسوب مع المحقق، يمكنه من تشغيل الحاسوب المراد تفتيشه إذا كان هذا الأخير محميا بكلمة مرور، ويجب أن يكون مزودا ببرنامج مضاعفة المساحة، فربما قام المتهم باستخدام هذا البرنامج مسبقا لمضاعفة مساحة القرص الصلب.

رابعا : برنامج معالجة الملفات كبرنامج (XTREE GOLD) : وهو برنامج معالجة آلية للملفات، في أي مكان على الشبكة، أو القرص الصلب، ويستخدم لتقسيم محتويات القرص الصلب الخاص بالمتهم، أو الأقراص المرنة المضبوطة ويستخدم لقراءة البرامج و الملفات في صورتها الأصلية.

خامسا : برنامج نسخ البيانات كبرنامج (LAP LINK) : هو برنامج يمكن المحقق من نسخ كل البيانات من حاسوب المتهم إلى قرص آخر، من خلال تقنية المنفذ المثالي أو المنفذ الموازي، وهو برنامج مفيد جدا يسمح بنسخ المعطيات بكل أمان ودقة قبل أي محاولة لتدميرها.

سادسا: برامج فحص الشبكة: هي أدوات تستخدم في فحص البرتوكول TPC/IP لمعرفة المشكلات المتعلقة بالشبكات و العمليات التي تعرضت لها، ويرجع فعاليتها إلى قدرتها على دخول الشبكات وتحديد نوع برامج التجسس و الفيروسات التي استعملت في عمليات الاختراق و تحديد مصدرها بدقة[1].

ومن بين هذه الأدوات:

---

[1]- عبد الله بن سعود بن محمد السراني- مرجع سابق- ص 55.

1. أداة (ARP) وظيفتها تحديد مكان الحاسوب على الشبكة.
2. برنامج (VISUAL ROUTE) وهو برنامج يلتقط أي كلمة لعملية ضد الشبكة فيبين وقت وزمن الهجوم ومصدره.
3. أداة (TRACER) هو برنامج يعمل على رسم مسار بين حاسوب الجاني و العناوين التي زارها و الفترات التي قضاها هناك.
4. أداة (NAT SAT) هو برنامج يعرض حالة الاتصال الحالية ومنافذ التصنت في شكل عرض كامل[1].

إضافة لذلك يستعين المحققون بنوع آخر من البرامج كبرامج عرض الملفات بكل أشكالها وصورها ، إضافة إلى إعادة تشكيلها عبر ما يعرف بالاستعانة بتقنيات الذكاء الاصطناعي، فجمع الأدلة في مجال الجرائم المعلوماتية يعتمد على تقنيات خاصة ومدى نجاعتها، فهي السبيل لحصر الاحتمالات و الأسباب و الفرضيات، وهي تتم عن طريق عمليات حسابية يقوم بها الحاسوب وفق برامج مصممة لذلك، تعمل على حصر الاحتمالات ثم إقصاء الأضعف منها وصولا إلى الاحتمال الأقوى[2].

سابعا : برامج كشف الفيروسات وتدميرها: يحب على المحقق أن يحمي أدواته وحاسوبه الخاص بالتحقيق، بواسطة برامج كشف الفيروسات فقد يعمد المتهم إلى تفخيخ حاسوبه بالفيروسات التي تنتقل إلى حاسوب المحقق وتدميره بمجرد ربطه بحاسوب المتهم لنسخ البيانات[3].

ويبقى أمر استقصاء الوسائل التي تعمل بها الجهات المختصة بالبحث و التحقيق في الجرائم المعلوماتية أمرا مستحيلا نظرا لخصوصية وسائلهم وبرامجهم التي تتميز بطابع السرية، فهي معدة

---

[1]- علي عدنان الفيل- مرجع سابق- ص 75-76

[2]- خالد عياد الحلبي-مرجع سابق- ص 214.

[3]- حسن طاهر داود- مرجع سابق- ص 229-230.

خصيصا لهم و لا يحق ترويجها خارجا، وذلك راجع إلى الخوف عليها من مكر المجرمين المعلوماتيين الذين يجتهدون في وضع خطوات استباقية ضد إجراءات البحث و التحقيق المعلوماتي.

الفرع الثالث: الأساليب الخاصة في التعامل مع الأشخاص ذوي العلاقة بالجريمة المعلوماتية.

نعني بالتحقيق مع الأشخاص ذوي العلاقة مع الحاسوب، تلك الإجراءات المتعلقة بتدوين أقوال الشهود، واستجواب المتهمين وإجراءات مواجهة المتهمين بالأدلة المتوفرة ضدهم وما يتبع ذلك من إجراءات مواجهة بين المتهمين بالأدلة المتوفرة من جهة، وبين المتهمين و الشهود من جهة أخرى، و العودة بالشهود و المتهمين إلى مسرح الجريمة عند الضرورة لمناقشتهم حول أجهزة الحاسوب وملحقاته[1].

الفقرة الأولى : أهمية إتباع أسلوب خاص في إستجواب المجرم المعلوماتي.

من أكبر المعوقات التي تقف حائلا في نجاح المحقق في استكمال المتطلبات الإجرائية الخاصة في مواجهة المتهم، هي شخصية المحقق في حد ذاته، و المتمثلة في التهيب من استخدام الحاسوب و الانترنت، إضافة إلى عدم اهتمامه بالمستجدات في مجال المعلوماتية.

إضافة إلى معوقات متعلقة بنقص المهارة الفنية للمحقق في التعامل مع الحاسوب و الانترنت، وعدم معرفة أساليب الجرائم المعلوماتية، وعدم الإلمام باللغة المعلوماتية لا سيما و أن هذا المجال غني واكتسب مصطلحات علمية خاصة أصبحت تشكل لغة خاصة لمحادثات و أساليب التفاهم بين المجرمين، ليس هذا وحسب بل اختصرت هذه المصطلحات بالعبارات و الحروف الأولى لتعرف باسم لغة المختصرات وهي لغة متطورة ومتجددة ، إذن يجب أن تتوفر في المحقق الخبرة الفنية و الكفاءة لأجل نجاحه في مجال التعامل مع مجرمي المعلوماتية[2].

---

[1]- محمد الأمين البشيري- التحقيق في الجرائم المستحدثة- مركز الدراسات و البحوث – جامعة نايف للعلوم الأمنية- الرياض- السعودية- سنة 2004- ص 120.

[2]- علي عدنان الفيل- مرجع سابق- ص 85.

عادة ما يطلق مجرمو المعلوماتية على أنفسهم صفة النخبة، (les élites) بحجة أنهم الفئة الأكثر معرفة بأسرار المعلوماتية، وعالم الحاسوب، وشبكة الانترنت ويطلقون على رجال السلطة القضائية ورجال القضاء صفة الضعفاء و القاصرين، نظرا لقلة خبرتهم ومعرفتهم بمجال النظم المعلوماتية، ولذلك فقد أصبحت توكل مهام التحقيق في الجرائم المعلوماتية لهيئات خاصة في هذا المجال، وشركات خاصة في مجال المعلوماتية، ويرى البعض أنه من الخطورة تخلي أجهزة العدالة و القضائية عن دورها في التحقيق في مثل هذا النوع من القضايا، لصالح الهيئات و الشركات الخاصة ،فبذلك ضياع لحقوق المجتمع تحت رحمة شركات خاصة همها الوحيد تحقيق الكسب المالي وهي غير مكلفة بتحقيق العدالة.

وحتى تكتمل قدرات الجهات الأمنية و القضائية في هذا الشأن، وجب الاستعانة بخبراء الحاسوب في كل مراحل البحث و التحقيق ، كما هو عليه الحال في التحقيق مع المتهمين و الشهود، إذ أن أخذ أقوالهم واستجوابهم يعتمد على منهجية معينة، وقدرات ومواهب لا تتوفر إلا لدى المحقق الذي اكتسب خبرة مهنية في مجال التعامل مع المجرمين إضافة إلى المعرفة الفنية للخبير في مجال المعلوماتية[1].

الفقرة الثانية : ضمانات الإستجواب .

يتولى عادة وفق التشريع الإجرائي الجزائي الجزائري قاضي التحقيق مهمة استجواب المتهم، وبذلك فهو إجراء ذو طابع قضائي لا يصح إلا من خلال احترام وتوافر الشروط المحددة قانونا و التي يمكننا إيجازها في النقاط التالية:

- الاستجواب إجراء من إجراءات التحقيق، يقصد من وراءه التحقق من شخصية المتهم ومناقشته مناقشة تفصيلية في التهمة المنسوبة إليه ومطالبته بالرد على الأدلة القائمة في مواجهته بنفيها أو التسليم بها ،

---

[1]- ضياء على أحمد النعمان- مرجع سابق- ص 377-378.

وهو بذلك إجراء يحقق وظيفتين الأولى إثبات شخصية المتهم ومناقشته بالأدلة و الثانية تحقيق دفاع المتهم من خلال فتح السبيل أمامه لتفنيذ الأدلة القائمة ضده، و بالتالي مساعدة القضاء على معرفة الحقيقة وكشف ملابسات وشخصية الفاعل الحقيقي[1] .

- يختلف استجواب المتهم عن مجرد سؤاله بواسطة أحد ضباط الشرطة القضائية خلال فترة البحث و التحري، ففي هذه الحالة يكون السؤال متعلق بالوقائع المنسوبة للمشتبه فيه فقط دون مناقشة تفصيلية ودون تحقيق لدفاع المشتبه فيه[2].
- يشترط لبدء الاستجواب استيفاء الشروط القانونية المنصوص عليها وفق قانون الإجراءات الجزائية و المقررة حسب نصوص المواد من 100 إلى 105 إضافة إلى التقييد بقواعد الموضوعية واحترام الكرامة الإنسانية للشخص المستجوب، وهي كلها ضمانات قانونية تضمن شرعية الإجراء، ولكن ما هي الضمانات التي تجعل من الاستجواب في الجرائم المعلوماتية إجراء كاشفا للحقيقة؟

الفقرة الثالثة: الأسلوب الأمثل لاستجواب مجرمي المعلوماتية.

إن التعامل مع الجريمة المعلوماتية بالبحث و التحقيق يتطلب وسائل خاصة و كذلك التعامل مع المجرم المعلوماتي في إطار استجوابه فيجب على قاضي التحقيق اتباع أسلوب خاص غير ذلك المعتاد في استجواب المتهمين في جرائم القانون العام الأخرى و يمكن حصر أسلوبه في مرحلتين:

أولا : قبل البدء في الاستجواب: قبل البدء في استجواب المتهم في الجريمة المعلوماتية وجب على قاضي التحقيق التقييد بالقواعد التالية:

---

[1]– عبد الفتاح بيومي حجازي– الجوانب الإجرائية لأعمال البحث والتحقيق الإبتدائي في الجرائم المعلوماتية– دراسة مقارنة على ضوء القواعد العامة للإجراءات الجنائية– مرجع سابق– ص 679.

[2]– المرجع السابق– ص 681.

1. تبادل المعلومات مع الخبير المعلوماتي من خلال تولي قاضي التحقيق مهمة شرح أهمية ترتيب المتهمين و طريقة توجيه الأسئلة إليهم، و كذلك يقوم الخبير شرح الأبعاد التقنية التي ينبغي استجلاءها من كل شخص موضع الاستجواب.

2. يزود الخبير قاضي التحقيق بكافة المصطلحات الضرورية التي يمكن استخدامها أثناء الحوار مع بيان معانيها للاستفادة منها عند الضرورة.

3. وضع خطة الاستجواب بناء على المعطيات السابقة.[1]

ثانيا : عند البدء في الاستجواب: تراعى عند البدء في أخذ أقوال المتهم من قبل قاضي التحقيق التعليمات التالية:

1. إتاحة فرصة حضور الخبير لجلسة الإستجواب، و منح هذا الأخير توجيه أسئلة فرعية وفق خطة مسبقة و كيفية متفق عليها مسبقا بمعرفة قاضي التحقيق.
2. يفضل في سبيل تحقيق التعاون بين الخبير و قاضي التحقيق أن يستعين الأول بأوراق يضعها أمام قاضي التحقيق تحدد وقت طرح السؤال و نوعه و موضوعه كما يمكن لقاضي التحقيق أن يتيح للخبير فرصة استجواب المتهم.
3. مراعاة القوانين الإجرائية التي تمنع بعضها حضور الخبير جلسة الاستجواب، و يستحب في هذه الحالة تشكيل لجان تحقيق من أجل ضمان حضور الخبير في عضويتها.
4. تفادي إضاعة الوقت في استجواب المتهم حول جريمة لا يمكن اكتشافها.
5. تحرير محضر الاستجواب بكل دقة و وضوح[2].

---

[1] – ضياء علي أحمد النعمان– مرجع سابق– ص 380.

[2] – محمد الأمين البشيرى– مرجع سابق– ص 123 ، 124.

إن استخلاص الدليل قد يكون من خلال استجواب المتهم كما يكون من خلال سماع الشهود، و لذلك كان على من يتولى أمر البحث و التحقيق في الجرائم المعلوماتية، إتباع قواعد خاصة في مجال سماع شهود الجريمة المعلوماتية.

الفقرة الرابعة: الشهادة في مجال الجريمة المعلوماتية.

تعرف الشهادة بصفة عامة بأنها أقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق أو القضاء بشأن جريمة وقعت سواء تتعلق بثبوت الجريمة و ظروف ارتكابها و اسنادها إلى المتهم أو براءته فيها ، و قد قال بشأنها بنتام (Bentham): " الشهود هم عيون القضاء و أذانها " و كثيرا ما يكون للشهادة أثناء جمع الاستدلالات أو التحقيق أكبر في الأثر في القضاء بالإدانة أو البراءة لأن الأقوال التي تتضمنها قد أدلي بها فور وقوع الحادث، قبل أن تمتد يد العبث إليها، أو قد يطول عليها الوقت فتضعف معالم الجريمة و الوقائع التي تنصب عليها[1].

و لا تقل أهمية الشهادة في مجال المعلوماتية عن نظيرتها في مجال الجرائم الأخرى، غير أن ما يمكن الإشارة إليه في موضوع الدراسة أن الشاهد المعلوماتي يختلف عن غيره من الشهود فهو صاحب معرفة علمية وتقنية بمجال المعلوماتية، و هو ما يفرض عليه التزامات من نوع خاص أمام جهة التحقيق.

أولا: المقصود بالشاهد المعلوماتي : سماع الشاهد إجراء كسائر إجراءات التحقيق في المواد التقليدية و هو أمر متروك لتقدير قاضي التحقيق و مرتبط بظروفه، و الأصل أن يطلب الخصوم سماع شهادة من يرون، و كذلك الحال لقاضي التحقيق الذي له أن يسمع شهادة أي شاهد يتقدم و لو من تلقاء نفسه و لو بدى له أنه لا يتحرى الصدق في أقواله[2].

---

[1] – عائشة بن قارة– مرجع سابق– ص 125.

[2] – عبد العال الدريبي– مرجع سابق– ص 312.

و الشاهد في مجال المعلوماتية هو ذلك الشخص صاحب الخبرة و التخصص في تقنيات الحاسوب ،و الذي له معلومات و مكاسب عن شبكات الحاسوب و الاتصال و الخدمات الخاصة بذلك ، إذا كانت مصلحة التحقيق تقتضي البحث عن الأدلة داخلها، و الشاهد المعلوماتي عدة أصناف يجوز لقاضي التحقيق استدعاء من شاء منهم لسماعه[1]:

1- القائم على تشغيل الحاسوب: و هو المسؤول عن تشغيل الحاسوب و المعدات المتصلة به و هو شخص تتوفر فيه الخبرة الكافية في مجال تشغيل الجهاز و استخدامه.

2- المبرمجون: و هم الأشخاص المختصمون في كتابة البرامج المعلوماتية و هم فئتان:

أ. مخططو برامج التطبيقات:يقوم هؤلاء بالحصول على خصائص و مواصفات النظام المعلوماتي المطلوب من محلل النظم ثم تحويلها إلى برامج دقيقة لتحقق هذه المواصفات.

ب. مخططو برامج النظم: يقوم هؤلاء بتصحيح و اختبار و تعديل برامج نظم الحاسوب الداخلية أي تلك الخاصة بالوظائف المتعلقة بتجهيز الحاسوب بالبرامج و الأجزاء الداخلية منه.

3- المحللون: هم فئة من الأشخاص مهمتهم تحليل الخطوات و جمع ببيانات النظام المعلوماتي ثم تحليلها، أي تقييمه لوحدات منفصلة و استنتاج العلاقات الوظيفية بين هذه الوحدات.

4- مهندسو الصيانة و الاتصالات : هم فئة المسؤولين عن أعمال الصيانة الخاصة بالحاسوب و الشبكات المتصلة به.

5- مديرو النظم: و هم من توكل لهم إدارة النظم المعلوماتية .[2]

و يبقى قاضي التحقيق الشخص الوحيد الذي له حرية استدعاء أيا كان منهم[3].

---

[1] - نزيهة مكاري- مرجع سابق- ص 75.

[2] -رضا هميسي- أحكام الشاهد في الجريمة المعلوماتية- بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة- 16و 17 نوفمبر 2015- كلية الحقوق – جامعة بسكرة- الجزائر ص 4،5.

[3] - يحصر قانون الدليل الخاص بولاية كاليفورنيا – الولايات المتحدة الأمريكية – شهود الجريمة المعلوماتية في:

- محل النظم الذي صمم البرنامج الذي نتج عنه الدليل.

ثالثا: التزامات الشاهد المعلوماتي : يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج إلى أنظمة تشغيل الحواسيب أو الشبكات، التي تحتوي على الأدلة الإجرامية غير أن هذا الطرح يبقى نسبيا نظرا للتوصيات المقدمة من قبل المؤتمر الدولي الخامس عشر للجمعية العامة لقانون العقوبات المنعقد بريو دي جانيرو – البرازيل – 2004 – و الذي أوصى بضرورة التعاون الفعال بين المجني عليهم و الشهود و غيرهم من مستخدمي التكنولوجيا المعلومات في سبيل مكافحة هذا النوع من الجرائم، و عليه فهل يجب على الشاهد في هذه الحالة مد يد العون و المساهمة بشكل أكبر في التحقيق أم يبقى ملتزم بقول الحقيقة ؟ و للإجابة عن هذه الإشكالية انقسم الفقه إلى اتجاهين:

1- **الاتجاه الأول:** يرى أنصاره أنه ليس من الواجب على الشاهد و حسب المنظور التقليدي لإلتزاماته، أن يقوم بطباعة البيانات المخزنة في ذاكرة الحاسوب و لا بتحليل ذاكرة النظام المعلوماتي، فهذا العمل الخبير و هو ما عمل به التشريع الألماني و التركي[1].

2- **الاتجاه الثاني:** يرى أنصاره أن الشاهد المعلوماتي يستطيع القيام بطبع المعلومات و تحليل البيانات و الكشف عن كلمات السر و هو ما أخذ به التشريع الفرنسي و الهولندي[2].

- المبرمج الذي قام بتحرير البرنامج و اختباره
- مشغل البرامج
- طاقم عمليات البيانات الذي يعد البيانات بالصورة التي يستطيع الحاسوب قراءتها.
- مهندسو الصيانة الإلكترونية.أنظر في ذلك : عبد العال الدريبي- مرجع سابق- ص 314.

[1] - عائشة بن قارة- مرجع سابق- ص 129 - 130.

[2] - عبد العال الدريبي- مرجع سابق- ص 316.

و لا يوجد في التشريع الجزائري ما ينص صراحة على أعباء الشاهد المعلوماتي فهو أمر متروك لقاضي التحقيق إن شاء أمر بذلك من عدمه، و قد تدعمت مساهمة الشهود في مجال أعمال مباشرة الدعوى العمومية و إجراءات التحقيق بصفة خاصة ، بما فيها في مجال الجرائم المعلوماتية بموجب التعديل الأخير لقانون الإجراءات الجزائية الجزائري الصادر بتاريخ 23 جويلية 2015 بموجب الأمر 02/15 و الذي نص في الفصل السادس منه على إجراءات حماية الشهود و الخبراء و الضحايا ، بموجب نصوص المواد من 65 مكرر 19 إلى 65 مكرر 28، على تعزيز دور الشاهد في مسار الإجراءات ، خصوصا إذا كانت المعلومات التي سيقدمها سببا في ظهور الحقيقة في الجرائم المنظمة و الإرهابية و جرائم الفساد ، من خلال منحه الحماية القانونية و الإجرائية في حال كان هناك تهديد يمس حياته أو سلامته الجسدية، أو سلامة أحد أفراد عائلته او أقاربه أو مصلحة أساسية له ، و ذلك من خلال إخفاء المعلومات المتعلقة بهويته ، تغيير مكان إقامته ، وضع خط هاتفي تحت تصرفه، تمكينه من نقطة إتصال مع مصالح الأمن ، ضمان حماية جسدية له ، وضع أجهزة تقنية وقائية بمسكنه ...إلــخ ، و هي كلها إجراءات تحفيزية تعزز دور الشاهد في الكشف عن ملابسات الجريمة بما فيها المعلوماتية.

إذا و في الأخير يمكننا القول بأن الإجراءات الخاصة بالبحث و التحقيق في مجال الجريمة المعلوماتية تتأثر حتما بالطبيعة الخاصة لهذه الجرائم، و يستحيل قطعا البحث و التحقيق بشأنها بواسطة الوسائل التقليدية، و لكن ذلك لا يمنع من اتخاذ الإجراءات الأخرى بشأنها كالأمر بالوضع تحت الرقابة القضائية أو الأمر بالحبس المؤقت هما من الإجراءات الضرورية في مجال الجريمة المعلوماتية، بالرغم من عدم امتيازها بخصائص نوعية ذات طابع معلوماتي فالهدف من البحث و الدراسة لجملة من الإجراءات دون غيرها راجع أولآ لخصوصيتها ، و ثانيا لنتائجها التي تقود المحقق إلى الحصول على الدليل أولا الالكتروني الذي يعتبر مفتاح فك شفرة الجريمة المعلوماتية ، فما هو يا ترى الدليل الإلكتروني؟ و ما هي خصائصه ؟ و عوائق إستخلاصه؟.

المبحث الثاني: نتائج البحث و التحقيق المعلوماتي و معوقاته.

تطورت وسائل التحقيق الجنائي في عصر المعلوماتية تطورا ملموسا يواكب حركة الجريمة، فبعد أن كان الطابع المميز لوسائل البحث و التحقيق يعتمد على وسائل تقليدية و أسلوب العنف و التعذيب لأجل الحصول على الدليل، أصبحت و في الوقت الراهن الوسائل العلمية هي أساس الوصول إلى الحقيقة، فأصبحت التقنية المعلوماتية هي التقنية الغالبة في مجال التحقيق الجنائي، و ذلك كنتيجة حتمية لتطور الأساليب الإجرامية و اعتمادها الأساليب التكنولوجية بالدرجة الأولى، على أساس أنها الطريقة الأمثل في تحصيل النتيجة الإجرامية.

إن الطبيعة الفنية و التقنية للجريمة المعلوماتية، نتج عنها و بالضرورة آثار و دلائل ذات طبيعة خاصة، و هو ما يطرح إشكالية شرعيتها في مجال الإثبات الجنائي، فالأدلة الناتجة عن الجريمة الإلكترونية أو ما يعرف بالأدلة الإلكترونية أو الرقمية، و هي بطبيعتها أدلة من نوع خاص، فهي عبارة عن نبضات إلكترونية بالدرجة الأولى تفتقر للمظهر المادي المميز لمفهوم الدليل الجنائي عادة، و هو ما جعلها محل تأويل فقهي و قانوني حول مدى مشروعيتها و قوتها الثبوتية أمام الجهات القضائية، غير أن هذه التأويلات ما فتأت أن تلاشت بفضل الاعتراف القانوني الذي حازت عليه من قبل أغلب النظم القانونية التي ساوت بينها و بين الأدلة التقليدية الغالبة في مجال الإثبات الجنائي.

و سنحاول في هذا المبحث استعراض المفاهيم العامة و الخاصة للدليل الإلكتروني باعتباره نتائج أعمال البحث و التحقيق في الجرائم المعلوماتية و ذلك من خلال إبراز تعريفه (المطلب الأول)، و تقدير قوته الثبوتية (المطلب الثاني)، و أهم العقبات التي تقف حائلا في مجال تحصيله (المطلب الثالث).

المطلب الأول: مفهوم الدليل الإلكتروني.

تعتمد الجرائم المعلوماتية في موضوعها على استخدام أساليب، التشفير و الرموز السرية، و التخزين الإلكتروني ... إلخ، و هي أساليب لا تترك ورائها آثارا مادية قد تكتشف أو يستدل من خلالها على الجناة، إن الطبيعة غير المرئية للأدلة المتحصل عليها من الجرائم المعلوماتية تلقي بظلالها، على الجهات التي تتعامل مع الجرائم التي تقع بالوسائل الإلكترونية، حيث تصعب قدرتهم على فحص و إختبار البيانات محل الاشتباه، و من ثم فقد سيتحيل عليهم الوصول للجناة، فمن المعلوم أن جهات البحث و التحقيق معتادة على جمع الدليل بالوسائل التقليدية للإثبات الجنائي التي تعتمد على الإثبات المادي للجريمة، لكن الأمر مختلف في محيط الإلكترونيات و المعلوماتية فلا مجال لتطبيق نفس الإجراءات[1].

فطبيعة الجريمة المعلوماتية لا تتوافق مع الدليل التقليدي فالقاضي لا يستطيع أن يبنى قناعته الكاملة في ظل وجود هذين المتغيرين غير المتوافقين، فلابد من توافق الجريمة مع طبيعة الدليل ، ففي مجال الجريمة المعلوماتية فإن الدليل الإلكتروني هو الدليل الملائم لأجل بناء قناعته ، فما هو يا ترى الدليل الإلكتروني و ما هي خصائصه و ما هي أنواعه، و من أين يمكن تحصيله؟

الفرع الأول: تعريف الدليل الإلكتروني و خصائصه : نتيجة للطفرة التي مست الجريمة و تحولها إلى معلوماتية، و ما صاحبها من تحول في نوع الدليل الجنائي من تقليدي مادي ، إلى مستحدث إلكتروني ، فإن هذا الأخير قد حظي بنوع خاص من الاهتمام الفقهي و القانوني من حيث تحديد مفهومه و خصائصه، نظرا لخصوصيتة و طبيعته الإلكترونية.

---

[1] – علي محمود حمودة-" الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي"- بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الإلكترونية – من 26 إلى 28 أفريل 2003- مركز البحوث و الدراسات- أكاديمية شرطة دبي- دبي- الإمارات العربية المتحدة – ص 08.

الفقرة الأولى: تعريف الدليل الإلكتروني.

أولا : التعريف اللغوي : يعرف الدليل لغة بأنه : ما يُستَدَلُّ به ، برهانٌ ، بيِّنة ، حجّة ، شاهد ، علامة.[1]

ثانيا : التعريف الإصطلاحي : أما إصطلاحا فهو ما يلزم من الفهم به شيء آخر، و غايته أن يتوصل العقل إلى التصديق اليقيني مما كان يشك في صحته أي التوصل نه إلى معرفة الحقيقة[2].

و قد وردت بشأن الدليل الإلكتروني عدة تعاريف أخرى فقد عرف على أنه: " الدليل الذي يجد له أساسا في العالم الافتراضي و يقود إلى الجريمة "، أو بأنه ذلك الجزء المؤسس على الاستعانة بتقنية المعالجة الآلية للمعلومات، و الذي يؤدي إلى إقناع قاضي الموضوع بثبوت ارتكاب شخص ما لجريمة عبر الأنترنت "[3].

و قد عرف كذلك بأنه: " المعلومات التي يقبلها العقل و المنطق و يعتمدها العلم، يتم الحصول عليها بإتباع إجراءات علمية و قانونية بترجمة المعلومات و البيانات المخزنة في الحاسوب و ملحقاته، و شبكات الاتصال و يمكن استخدامها في أي مرحلة من مراحل التحقيق و المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بالجريمة[4].

و قد نال الدليل العلمي حصة معتبرة من الاهتمام من قبل الهيئات الدولية و الخاصة المهتمة بموضوع الأدلة الإلكترونية فعرفته المنظمة الدولية لأدلة الحاسوب (IOCE) International Organisation of Computer Evidence. بأنه: " المعلومات المخزنة أو المتنقلة

---

[1] – قاموس المعاني الإلكتروني متوفر على شبكة الأنترنت – تاريخ التصفح 2014/11/01 – الرابط الإلكتروني المباشر :

http://www.almaany.com/ar/dict/ar-ar/الدليل/

[2] – عائشة بن قارة– مرجع سابق– ص 51.

[3] – ضياء علي أحمد النعمان– مرجع سابق– ص 282.

[4] – خالد عياد الحلبي– مرجع سابق– ص 230.

في شكل ثنائي فيمكن أن تعتمد عليها المحكمة " و هو نفس المعنى التعريفي المقدم من قبل الفريق العلمي العامل على موضوع الأدلة الرقمية[1]. Standard Working Group On Digital Evidence (SWGDE)

إذن من خلال ما سبق يمكننا إقتراح التعريف الخاص بنا على أن "**الدليل المعلوماتي أو الإلكتروني هو عبارة عن معلومات مستخلصة تكون مخزنة إما على جهاز الحاسوب نفسه، أو ملحقاته كالأقراص الصلبة الخارجية أو المدمجة، أو بطاقات الذاكرة، أو ذاكرة الطابعة أو متنقلة عبر الشبكات الاتصال ،و التي يتم التقاطها و تجميعها من أجل تحليلها و استرجاعها بواسطة برامج خاصة**" .

الفقرة الثانية: خصائص الدليل المعلوماتي.

يتميز الدليل المعلوماتي و بالنظر إلى البيئة التي ينشأ و يعيش فيها، و يحصل منها بمجموعة من الخصائص التي تميزه على الدليل المادي التقليدي يمكن حصرها في النقاط التالية:

أولا: الدليل الإلكتروني دليل علمي بالدرجة الأولى:يتكون الدليل الإلكتروني من بيانات و معلومات ذات صفة إلكترونية غير ملموسة و لا تدرك بالحواس العادية، بل يتطلب لإدراكها الاستعانة بالبرامج و الوسائل الخاصة بذلك[2]، و الدليل الإلكتروني كالدليل العلمي يخضع لقاعدة لزوم التجاوب مع الحقيقة كاملة وفق قاعدة (إن القانون مسعاه العدالة، أما العلم فمسعاه الحقيقة) إذن فبحكم الطبيعة الخاصة للدليل الإلكتروني فإنه لا يجب أن يخرج عما توصل إليه العلم الرقمي و إلا فقد معناه[3].

---

[1] – عائشة بن قارة– مرجع سابق– ص 54 – 55.
[2] – خالد عياد الحلبي – مرجع سابق– ص 231.
[3] – عائشة بن قارة– مرجع سابق– ص 62.

ثانيا: الدليل الإلكتروني دليل تقني : يستمد الدليل الإلكتروني هذه الخاصية من البيئة الرقمية، فيجب أن يكون مستوحى أو مستنبط من بيئته التي يعيش فيها، و هي البيئة الرقمية أو الإلكترونية و هو العالم الكامن في أجهزة الحواسيب و الشبكات[1].

ثالثا: الدليل الإلكتروني دليل يصعب التخلص منه : تعد هذه الخاصية من أهم خصائص الدليل الإلكتروني، فهي ما يميزه عن الدليل التقليدي، فيمكن للجاني التخلص و بكل سهولة من الأوراق التي تحمل إقراره بالذنب بحرقها، أو بمسح موضوع البصمات أو التخلص من الشهود، أما بالنسبة للأدلة الإلكترونية فإنه يمكن استرجاعها حتى بعد أتلافها أو محوها، و ذلك بالاستعانة ببرامج خاصة على شكل برنامج (RECOVER LOST DATA) حتى و إن استعمل الجاني أمر المحو (DELATE) أو أمر إعادة تشكيل القرص الصلب باستخدام تقنية (FORMAT) سواء كانت هذه البيانات صورا أو رسومات أو كتابات أو غيرها[2].

رابعا: الدليل الإلكتروني قابل للنسخ : يمكن استخراج نسخ من الدليل الإلكتروني بصفة مطابقة للأصل و لها نفس القيمة العلمية و الحجية الثبوتية التي لا تتوافر في الدليل التقليدي، مما يجعل منه ضمانة شديدة الفعالية للحفاظ على الدليل من مخاطر التلف و التغيير[3].

خامسا: الدليل الإلكتروني سجل خاص بتحركات المتهم: فهو يرصد و يسجل معلومات عن الجاني و يحللها في ذات الوقت فيسجل تحركاته و سلوكياته و بعض المعلومات الشخصية عنه و هو ما يجعل منه معيارا مفيدا في مجال البحث الجنائي[4].

---

[1] – ضياء علي أحمد النعمان– مرجع سابق– ص 294.

[2]– سامية بلجراف – سلطة القاضي الجنائي في قبول و تقدير الدليل الرقمي– بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة– 16و 17 نوفمبر 2015– كلية الحقوق – جامعة بسكرة– الجزائر ص 5.

[3] – خالد عياد الحلبي– مرجع سابق– ص 232.

[4] – عائشة بن قارة– مرجع سابق– ص 64.

إذن فالدليل الإلكتروني نوع خاص من الأدلة الجنائية بالنظر إلى خصوصية الرقمية و التي تميزه عن الأدلة التقليدية بصفة كلية و تجعل منه الدليل الأنسب في مجال البحث و التحقيق في الجرائم المعلوماتية.

الفرع الثاني: شروط صحة الدليل المعلوماتي.

إن الأدلة الإلكترونية إما أن تكون مخرجات ورقية يتم إنتاجها بواسطة الطابعة أو غير ورقية أي أن تكون (غير) إلكترونية كالبيانات المخزنة على الأقراص الصلبة أو الأقراص المضغوطة أو غيرها من الأشكال الإلكترونية، و قد تتمكن في شكل عرض على الشاشة الخاصة بالحاسوب، سواء كانت مخزنة على ذاكرة الحاسوب أو على شبكة الانترنت و يكون الدليل الإلكتروني غير قابل للتعامل نه إذا ما شابه البطلان فلا يصح الاستناد عليه[1].

و يرى البعض من الفقه " أن المقصود بحجية الدليل الإلكتروني هو قيمة ما يتمتع به هذا الدليل بأنواعه المختلفة من قوة استدلالية على صدق نسبة الفعل الإجرامي إلى شخص معين " و لقبول الدليل الإلكتروني كأساس تشيد عليه الحقيقة سواء أ كان الحكم الصادر يوحي بالأدلة أو البراءة فإنه يجب إن يتوفر في هذا الدليل عدة شروط هي[2]:

---

[1] – علي حسن أحمد الطوالبة– "مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي" – بحث منشور على الموقع الإلكتروني لمركز الإعلام الأمني– أكاديمية الشرطة البحرينية– مملكة البحرين– أفريل 2011– ص 2–تاريخ التصفح : 2014/05/29– الرابط الإلكتروني:

http://www.policemc.gov.bh/reports/2011/April/13-4-2011/634383168746341670.pdf

[2] – ضياء علي أحمد النعمان– مرجع سابق– ص 294.

الفقرة الأولى: يجب أن يكون الدليل الإلكتروني متحصلا بطريقة مشروعة.

يقصد بالشرعية في المقام الأول عدم مخالفة الأحكام التي تهدف إلى صيانة كرامة الإنسان و حماية حقوقه، و لذلك تتضمن الدساتير الحديثة قواعد أساسية تضبط مسائل التفتيش و التوقيف و الحجز و الحبس و غيرها، بحيث يتقيد بها المشرع عند وضع قانون الإجراءات الجزائية ، فكل دليل مستمد بصفة مخالفة لهذه الأحكام يعتبر باطلا بطلانا مطلقا.[1].

و قد عرف الفقه المشروعية بأنها: " التوافق و التقيد بأحكام القانون في إطاره و مضمونه العام فهي تهدف إلى تقرير ضمانه أساسية و جدية للأفراد، لحماية حرياتهم و حقوقهم الشخصية ضد تعسف السلطة من التطاول عليها في غير الحالات التي رخص فيها القانون بذلك من أجل حماية النظام الاجتماعي و تحقيق حماية للفرد ذاته.

و يعني مبدأ مشروعية الدليل الجنائي الإلكتروني بما يتضمنه من مفاهيم الإلكترونية ، ضرورة إتفاق الإجراء مع القواعد القانونية و الأنظمة المتبعة في وحدات المجتمع المتحضر، أي أن قاعدة مشروعية الدليل الجنائي لا تقتصر فقط على مجرد المطابقة مع القاعدة القانونية ، بل يجب أن تراعي المبادئ السامية لحقوق الإنسان و قواعد النظام و حسن الآداب في المجتمع ، فإذا كانت المعلومات التي تشكل جريمة مخزنة في ذاكرة الحاسوب أو على الأقراص الصلبة أو المرنة فإن التساؤل الذي يدور حول مدى إمكانية الحصول عليها من المتهم نفسه أو من غيره إذا كان يعلم سبيل الوصول إليها بإرادته أو من خلال إجباره على ذلك؟ إن الإجابة عن هذا التساؤل دفعت بالفقه إلى اتخاذ موقفين:

---

[1]– علي حسن أحمد الطوالبة– التفتيش الجنائي على نظم الحاسوب و الانترنت – دراسة مقارنة– مرجع سابق– ص 184.

الاتجاه الأول: يرى أنه لا يجوز إجبار المتهم على طباعة ملفات بيانات مخزنة داخل نظامه المعلوماتي، أو إلزامه بالكشف عن الثغرات أو كلمات السر الخاصة بالدخول عملا بمبدأ أنه لا يجوز إلزام الشخص بإتهام نفسه[1] .

أما بالنسبة للشهود فإن أنصار هذا الاتجاه يرون بأن الشاهد غير مجبر على تقديم المساعدة للحصول على الدليل الإلكتروني، كما هو الحال عليه في لوكسمبورغ أين يتمتع الشاهد بحرية الرفض عن الإجابة أمام المحكمة عن كل ما يعرفه، و بالتالي يصعب إجباره على تقديم بيانات معلوماتية بصفة قادرا على الوصول إليها نظرا لمعرفته كلمة السر، أما إن تعاون من تلقاء نفسه فذلك لا يعدم أن يكون أقرب للخبرة منه للشهادة[2].

الاتجاه الثاني: يوافق الرأي الأول من حيث عدم جواز إجبار المتهم على إدانة نفسه غير أن له موقفا آخر تجاه التزامات الشاهد، فيرى أن من التزامات الشاهد طبع ملفات البيانات و الإفصاح عن كلمة السر، ما عدا الحالات المتعلقة بالمحافظة على سر المهنة فإنه يكون حرا في الالتزام بأداء الشهادة و كما هو الحال في فرنسا إضافة إلى هولندا التي يحفز قانون الحاسوب فيها سلطات التحقيق إصدار أمر للقائم بتشغيل النظام من أجل تقديم المعلومات اللازمة الخاصة إما بالإفصاح عن كلمات المرور السرية، الشفرات الخاصة بتشغيل البرامج[3].

و يبقى أمر تفادي الطرق غير المشروعة في تحصيل الدليل الإلكتروني أمرا ضروريا كاستخدام التعذيب، الإكراه المادي أو المعنوي، إطالة التحقيق ،استعمال مصل الحقيقة، التنويم المغناطيسي الغش، التدليس تجاه المتهم من أهم ضمانات مشروعية الدليل الإلكتروني.

---

[1] – ضياء علي أحمد النعمان– مرجع سابق– ص 313 – 314.
[2] – علي حسن أحمد الطوالبة– التفتيش الجنائي على نظم الحاسوب و الانترنت– دراسة مقارنة– مرجع سابق–ص 186.
[3] – علي حسن أحمد الطوالبة–" مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي"– مرجع سابق– ص 5.

الفقرة الثانية: أن يكون الدليل الإلكتروني ذا علاقة بموضوع الجريمة المعلوماتية.

نصت على ضرورة توافر هذا الشرط المادة 407 من قانون الإثبات الفدرالي الأمريكي، و أسمته بمبدأ العلاقة الكاشفة حيث يتطلب ضرورة أن تكون هناك علاقة ما بين الدليل و ما بين الواقعة محل الدعوى، و هو مبدأ لا يتحقق إلا بتحقق شرط آخر، و هو مطابقة الدليل الإلكتروني المستخرج من الحاسوب للأصل المخزن بداخله[1].

الفقرة الثالثة: أن يكون الدليل الإلكتروني يقيني غير قابل للشك.

يشترط في الأدلة الإلكترونية أن تكون غير قابلة للشك حتى يمكن الحكم بالإدانة، ذلك أنه لا مجال لدحض قرينة البراءة و افتراض عكسها،إلا عندما يصل القاضي إلى درجة من القناعة تتسم بالجزم و اليقين[2].

و اليقين في النظم الإجرائية هو عبارة عن حالة ذهنية أو عقلانية تؤكد وجود الحقيقة و يتم الوصول إلى ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من وقائع الدعوى و ما يتطبع في ذهنه من تصورات و احتمالات ذات درجة عالية من التأكيد و يمكن الوصول إلى اليقين عن طريق نوعين من المعرفة إحداهما حسية تدرك بالحواس، و الأخرى معرفية تدرك بالعقل عن طريق التحليل و الاستنتاج[3].

و تأكيدا لمبدأ يقينية الدليل الإلكتروني فقد أكد الفقه في كندا على اعتبار مخرجات الحاسوب من أفضل الأدلة لذا فإنها تحقق اليقين المنشود في الأحكام الجنائية ، كما نصت بعض القوانين في الولايات

---

[1] – ضياء علي أحمد النعمان– مرجع سابق– ص 315.
[2] – سامية بلجراف –مرجع سابق–ص 9.
[3] – ضياء علي أحمد النعمان– مرجع سابق– ص 313.

المتحدة الأمريكية على أن النسخ المستخرجة من البيانات التي يحتويها الحاسوب تعد من أفضل الأدلة المتاحة لإثبات هذه البيانات و بالتالي يتحقق مبدأ اليقين لهذه الأدلة[1].

الفقرة الرابعة: قابلية الدليل الإلكتروني للمناقشة.

يقصد بهذا الشرط وجوب مناقشة الدليل الجنائي بصفة عامة أي أن القاضي لا يمكن له أن يؤسس قناعته إلا على العناصر الإثباتية التي طرحت للمناقشة في جلسات المحاكمة، و خضعت لحرية مناقشة أطراف الدعوى و هو ما يعني أن الأدلة الإلكترونية سواء المتحصل عليها من الحاسوب أو من شبكة الأنترنت سواء أكانت مطبوعة أم بيانات معروضة على الشاشة أو مخزنة على دعامة يجب أن تكون محل مناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة و بناءا على ذلك فإن كل دليل تم الحصول عليه من خلال البيئة الرقمية يجب أن يعرض في الجلسة بصفة مباشرة أمام القاضي، و هذا ما ينطبق على الشهود الذين يجب أن يعيدوا أقوالهم مرة أخرى أمام المحكمة، و كذلك الخبراء و ذلك لأجل مناقشة تقاريرهم التي خلصوا إليها[2].

وما تجدر الإشارة إليه هو أن القاضي ولكي تكون له السيادة والهيمنة على الدعوى الجنائية فيجب أن يكون متدربا على كيفية التعامل مع تقنية المعلوماتية وتعقيداتها بشكل واف حتى يضمن له هذا التأهيل العلمي لنجاح مهمته.[3]

إذن فالدليل الإلكتروني و بحسب ما إستعرضناه هو دليل على قدم المساواة مع باقي أنواع الأدلة الجنائية ، بالرغم من مميزاته و خصائصه غير المألوفة في مجال الإثبات الجنائي ، و ذلك ما يمكن

---

[1] – علي حسن أحمد الطوالبة– "مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي"– مرجع سابق– ص 8.

[2] – علي حسن أحمد الطوالبة– التفتيش الجنائي على نظم الحاسوب و الانترنت– دراسة مقارنة– مرجع سابق–ص 193.

[3] – ضياء علي أحمد النعمان– مرجع سابق– ص 312.

تفسيره بأنه متناسب و الجريمة الناشئ عنها التي تتميز هي الأخرى بمميزات و خصائص تخرج عن ما ألفناه بشأن الجرائم التقليدية المادية ، و لكن يبقى تقدير حجته و قوته الثبوتية في مجال الإثبات الجنائي من أهم المسائل التي تؤثر على مصداقية أعمال البحث و التحقيق في مجال الجرائم المعلوماتية و هو ما سنحاول إستعراضه في المطلب الموالي.

المطلب الثاني: حجية الدليل الإلكتروني في نطاق الإثبات الجنائي.

بعد إستنفاذ رجال البحث والتحقيق لأعمال جمع الدليل الإلكتروني الناشئ عن الجريمة المعلوماتية ، بإعتباره ختام مرحلة البحث والتحقيق الجنائي وأساس مرحلة المحاكمة التي يكون من خلالها هذا الدليل محل مناقشة من قبل الخصوم (النيابة– المتهم) وتحليل وتمحيص من قبل هيئة الحكم (القاضي) ، فإنه و من دون شك يعتبر الدليل الجنائي العنصر الأهم والأساسي لتحديد مصير المتهم بين الحكم بإدانته أو براءته ، بالنظر إلى مدى حجيته في نطاق الإثبات الجنائي ومدى إعتماد القانون هذه الحجية، فالدليل الإلكتروني الناتج عن أعمال البحث والتحقيق وكما سبق ورأينا، ذو طبيعة خاصة فهو رقمي إلكتروني بالدرجة الأولى ، ويختلف تماما عن الأدلة المادية التقليدية التي ألف القضاء التعامل معها بإختلاف أنظمتها، وهو ما يطرح إشكالية مدى قابلية القضاء للتعامل مع هذا النوع من الأدلة المستحدثة، ومدى إقرار الأنظمة القانونية بحجية هذا النوع من الأدلة؟

إن الإجابة عن هذا التساؤل يقتضي التعرض إلى مواقف القوانين المختلفة في التعامل مع الدليل الإلكتروني، وهي الأنظمة المصنفة ما بين لاتينية(الفرع الأول) وأنجلوساكسونية (الفرع الثاني) ، مع التعرض ختاما إلى موقف المشرع الجزائري إزاء هذه الإشكالية المستحدثة (الفرع الثالث).

الفرع الأول: حجية الدليل الإلكتروني في الأنظمة اللاتينية.

تتعامل الأنظمة القانونية مع الأدلة الجنائية بشكل متباين ، بين التضييق و التقييد ، إلى التوسع و الإطلاق ، و لذلك فقد تم إعتماد تقسيم ثنائي للأنظمة القانونية في هذا المجال ، بين لاتينية و أنجلوساكسونية ، و ذلك كناية بالدول التي تتبنى إحدى النظامين ، و سنستعرض بدءا مسألة حجية الدليل الإلكتروني بالنسبة للدول التي تتبنى النظام اللاتيني .

الفقرة الاولى : نظام الإثبات الحر أساس النظم اللاتينية في الإثبات.

تعتمد هذه الأنظمة مبدأ حرية الإثبات، ومنه فإن للقاضي سلطة قبول جميع الأدلة فيستطيع الأخذ بالإعتبار جميع أنواع الأدلة، ثم تقييم مدى إعتماد المحكمة على تلك الأدلة، وبالتالي فإن جميع طرق الإثبات مقبولة ما لم يلغي المشرع بعضها صراحة ، إن هذه الأنظمة لا تتردد في قبول تقديم سجلات الحاسوب كدليل للإثبات.[1]

فالأنظمة اللاتينية تأخذ بالأدلة المعنوية في الإثبات بحيث يترك للأطراف المتنازعة حرية تقديم الأدلة التي تدعم مواقفهم أو تشخص الوقائع المنسوبة إليهم ، ويعمل القاضي على فهمها وتقدير قيمتها الثبوتية ولا يخضع في ذلك لرقابة قاضي النقض ولكن ذلك لا يعني أن سلطته غير محدودة بل هو مقيد بفحص ومراقبة ونزاهة هذه الدلائل، ومتى أغفل ذلك أدى إلى هدر هذه الدلائل.[2]

---

[1] – ممدوح عبد الحميد عبد المطلب– مرجع سابق– ص 128.

[2] – محمد أزيلاجي– "حجية دليل الحاسوب الآلي في النطاق الجنائي"– مقالة منشورة بالمجلة المغربية للمنازعات القانونية– عدد مزدوج 10–11– سنة 2010– دون ذكر هيئة النشر –وجدة– المملكة المغربية– ص 46-47.

الفقرة الثانية : النظم اللاتينية ومسألة الإثبات بالدليل الإلكتروني.

يتصدر النظم القانونية التي تتبنى نظام الإثبات الحر و تحت وصف النظم اللاتينية ،كل من فرنسا وبلجيكا ومصر، وبالنسبة لهذه التشريعات فإن حجية الأدلة الإلكترونية لا تثير صعوبات نظرا لحرية تقديم هذه الأدلة لإثبات الجرائم المعلوماتية إضافة إلى سلطة القاضي الجنائي في تقدير هذه الأدلة ذات الصيغة الخاصة بإعتبارها أدلة إثبات في المواد الجنائية.[1]

ونتيجة لهذا فإنه يحظر على المشرع إضفاء قوة معينة لأي دليل من شأنه أن يقيد سلطة القاضي في تكوين قناعته الشخصية أو يطبع على بعضها شكا أو عدم ثقة أي يستبعدها القاضي من تقديره.[2]

وما يمكن الإشارة إليه أنه في النظام الحر للإثبات تكون جهة الإتهام ملزمة بإقامة الدليل على ثبوت الجريمة في حق المتهم، ما لم تكن هناك قيود تتعلق بأدلة قانونية أو قيود على المتابعة وفي غير ذلك يكون الأطراف أحرار في تقديم الأدلة.

أولا: في فرنسا: لطالما أعتبر الفقه الفرنسي مشكلة مدى قبول الدليل الإلكتروني في مجال الإثبات الجنائي من المسائل غير المستعجلة، فالأساس هو حرية القاضي في تقدير هذه الأدلة فقد اعترف الفقه في فرنسا بالدليل الإلكتروني، و صنفه من قبيل الأدلة الناشئة عن الآلة أو الأدلة العلمية ،وهو ما قضت به محكمة النقض الفرنسية.[3]

أما من الناحية القانونية فقد أقر المشرع بمبدأ حرية الإثبات الجنائي صراحة بمقتضى المادة 427 من قانون الإجراءات الجزائية الفرنسي، و التي جاء فيها ما لم يرد نص مخالف "يجوز إثبات

---

[1] – علي حسن أحمد الطوالبة– التفتيش الجنائي على نم الحاسوب والأنترنت– دراسة مقارنة– مرجع سابق– ص 196.
[2] – عائشة بن قارة– مرجع سابق –ص 183.
[3] – علي حسن أحمد الطوالبة–" مشروعية الدليل الإلكتروني المستمد من التفتيش"– مرجع سابق– ص 11.

الجرائم بجميع طرق الإثبات ويحكم القاضي بناء على اقتناعه الشخصي " ، وإن كان هذا النص مخصصا لمحاكم الجنح إلا نه يجوز تطبيقه على كافة المستويات وهو المبدأ الذي حرصت محكمة النقض الفرنسية على التشديد على إحترامه، بل وقد أكدت الدائرة الجنائية لمحكمة النقص الفرنسية على ضرورة قبول أي دليل مقدم ما لم يكن مستثنى بنص القانون ولو كان ذلك الدليل غير مشروع ، وهو ما يعزز إتجاه التشريع الفرنسي في الأخذ بالدليل الإلكتروني.[1]

ثانيا: في بلجيكا : يأخذ التشريع البلجيكي بنظام الإثبات الحر في ميدان الأدلة الناتجة على الجرائم المعلوماتية ،وذلك طبقا لنص المادة 461 من قانون العقوبات ويعد الحكم الصادر عن المحكمة (AVERS) في 1984/12/13 أول حكم صادر في هذا الخصوص بحيث أعتبر قيام المتهم بنسخ ثلاث (03) نسخ عن برامج تعود ملكيتها للشركة فعلا مجرما تنطبق عليه العقوبة المقررة لذلك، وهو ما فتح الطريق أمام تبني القضاء البلجيكي لنظام الإثبات الحر فيجوز الأخذ بالدليل الإلكتروني.[2]

ثالثا: في مصر : كرست المادة 291 من قانون الإجراءات الجنائية المصري مبدأ إعمال النظام الحر للإثبات الجنائي بما فيها الإعتماد على الدليل الإلكتروني بحيث جاء فيها أن للمحكمة أن تأمر ولو من تلقاء نفسها أثناء نظر الدعوى بتقديم أي دليل تراه لازما لظهور الحقيقة ، وهو ما أكدته محكمة النقض المصرية في العديد من أحكامها بالقول بأن القانون وفيما عدا ما إستلزمه من وسائل خاصة للإثبات فتح الباب أمام القاضي على مصرعيه يختار من كل طرقه ما يراه موصلا إلى الكشف عن الحقيقة ويزن قوة الإثبات المستمدة من كل عنصر.[3]

---

[1] – عائشة بن قارة– مرجع سابق– ص 185.

[2] – محمد أزيلاجي– مرجع سابق– ص 48.

[3] – عائشة بن قارة– مرجع سابق– ص 187.

الفقرة الثالثة : نتائج إعمال مبدأ نظام الإثبات الحر في مواجهة الدليل الإلكتروني.

أولا – الدور الإيجابي للقاضي الجنائي في توفير الدليل الإلكتروني: إن إعمال مبدأ نظام الإثبات الحر وكما يمنح للأطراف حرية تقديم الأدلة التي يرونها مناسبة إما لإثبات الإدانة أو دحض التهم، بما فيها الدليل الإلكتروني الذي يعتبر على قدم المساواة مع باقي الأدلة الأخرى فإنه يمنح للقاضي دورا أكثر إيجابية في توفير الدليل الإلكتروني ، و يقصد به عدم التزام القاضي بما يقدم إليه من قبل أطراف الدعوى من أدلة فحسب ، بل يجب عليه أن يبادر من تلقاء نفسه إلى إتخاذ جميع الإجراءات لتحقيق في الدعوى والكشف عن الحقيقة الفعلية ، ذلك لأن الحقيقة لا تظهر من تلقاء نفسها وإنما هي في حاجة دوما إلى من يبحث وينقب عنها، وليس له ان يقتنع بما يقدم إليه من أطراف الدعوى وإنما عليه أن يبحث من تلقاء نفسه عن الأدلة اللازمة لتكوين عقيدته على الوجه الصحيح.[1]

وهو ما يستشف من نص المادتين 442 – 536 من قانون الإجراءات الجزائية الفرنسي التي تتيح لمحاكم المخالفات والجنح أن تتخذ جميع الإجراءات الضرورية لتكوين قناعتها فلها أن تسأل المتهم حول أسس الاتهام، وتستمع للشهود وتستدعي الخبراء إذا ما واجهتها مسألة فنية، أما بالنسبة لمحكمة الجنايات فنص المادة 310 من نفس القانون يمنح لرئيس المحكمة سلطة تقديرية خاصة للقيام بجميع الإجراءات التي تقدر فائدتها في كشف الحقيقة وهو ما يقابلها في القانون المصري نص المادة 291 من قانون الإجراءات الجزائية.

إذن فالدليل الإلكتروني أمام الأنظمة اللاتينية دليل يتمتع بكل قوته الثبوتية ما دام مشروعا وتتوفر فيه الشروط التي أسلفنا ذكرها في المطلب الأول، مهما كانت طبيعة وشكله وصورة تقديمه أمام الجهات

---

[1] – عائشة بن قارة– مرجع سابق– ص 189، 190.

القضائية غير أن هذا الإعتراف بالقوة الثبوتية للدليل الإلكتروني لا يلاقي نفس درجة القبول على مستوى التشريعات الأنجلوساكسونية.

الفرع الثالث : حجية الدليل الإلكتروني أمام الأنظمة الأنجلوساكسونية .

يقصد بالأنظمة الأنجلوساكسونية، الأنظمة القانونية المتبعة من قبل دول المملكة المتحدة والولايات المتحدة الأمريكية وباقي الدول المتأثرة بهذين النظامين .

الفقرة الأولى : أساس مبدأ الإثبات للأنظمة الأنجلوساكسونية .

وفقا لهذا النظام فإن المشرع هو الذي يحدد حصرًا الأدلة التي يجوز للقاضي اللجؤ إليها في الإثبات، كما يحدد القيمة الإقناعية لكل دليل ، بحيث يقتصر دور القاضي على مجرد فحص الدليل للتأكد من توافر الشروط التي حددها القانون ، فلا سبيل للاِستناد إلى أي دليل لم ينص عليه القانون صراحة ضمن الأدلة المحدّدة على سبيل الحصر ، كما أنه لا دور للقاضي في تقدير القيمة الإقناعية للدليل ، ولهذا سمي هذا النظام بنظام الإثبات القانوني ، حيث أن القانون قيد القاضي بقائمة من الأدلة التي حدّدت قيمتها الاِثباتية ، وهذا النظام يسود الدول الأنجلوساكسونية ، كالمملكة البريطانية والولايات المتحدة الأمريكية ، ولذا فإن النظم التي تتبنّى هذا النظام لا يمكن في ظلها الاِعتراف للدليل الإلكتروني بأي قيمة إثباتية ما لم ينص القانون صراحة على ذلك ، ومن ثم فإنه لا قيمة للدليل الإلكتروني مهما حاز على شروط اليقين ما لم ينص عليه القانون ، فيحكم القاضي بما يخالف قناعته التي تكونت لديه من أدلة غير معترف بها. [1]

---

[1]– خالد عياد الحلبي – مرجع سابق – ص 236 ، 237 .

الفقرة الثانية : مشكلة قبول الدليل الإلكتروني في ظل الأنظمة الأنجلوساكسونية.

تطرح على مستوى الأنظمة الأنجلوساكسونية إشكالية مدى قبول الدليل الإلكتروني في مجال الإثبات الجنائي لتعارضه مع أحد أهم مبادئ الإثبات التي تحكم هذه النظم وهي :

أولاً : تعارض الدليل الإلكتروني وقاعدة اِستثناء أو اِستبعاد شهادة السماع : تحكم قاعدة اِستبعاد شهادة السماع نظام الإثبات موضوع الأدلة المقدمة ، ويعتبر الدليل الإلكتروني حسب مفهوم هذه القاعدة شهادة سماع ، فهو يتكون من جمل وكلمات أدخلها شخص إلى جهاز الحاسوب سواء تمّ معالجة تلك البيانات أم لا ، و قام شخص أخر بإعادة إستخراجها ،هو ما من شأنه أن يثيرًا اِعتراضًا على قبول المستندات المطبوعة التي يخرجها الحاسوب في الإثبات أمام القضاء الجنائي .

ثانيا : تعارض الدليل الإلكتروني وقاعدة المحرّر الأصلي : بالنسبة لكيفية تقديم الأدلة وعرضها على القضاة، تحكم قاعدة المحرّر الأصلي النظم الأنجلوساكسونية ، أي عدم الأخذ بالنسخ المطابقة للأصل ، وإذا ما طبقنا هذه القاعدة على الدليل الإلكتروني فإنها ستؤدي وبدون شك إلى اِستبعاده من نطاق الإثبات ،باعتبار مخرجات الحاسوب نسخًا لا أصلا ، وذلك لأن عرض الدليل الإلكتروني أمام القضاء يكون في شكل مستندات مطبوعة، أو بيانات معروضة على الشاشة ، والأصل أن بيانات الحاسوب هي مجرد إشارات ونبضات ممغنطة وليست مرئية للعين البشرية ، مما لا يتيح للمحلفين والقضاة وضع اليد عليها لأجل معاينتها، وهو ما يجعل الأدلة الإلكترونية المقدمة نُسخا أي أدلة ثانوية لا أصلية .[1]

1- عائشة بن قارة – مرجع سابق – ص 196 – 197.

الفقرة الثالثة : الحلول القانونية و الفقهية لمشكلة حجية الدليل الإلكتروني في نظم الولايات المتحدة الأمريكية والمملكة البريطانية.

أمام التعارض الواضح بين المبادئ الأساسية التي تحكم نظم الإثبات الجنائي في النظم الأنجلوساكسونية، وطبيعة الدليل الإلكتروني كان على الدول التي تتبنى هذا النظام إيجاد الحلول في مواجهة هذا التعارض، على اعتبار أنها الدول التي تشهد الانتشار الواسع للجرائم المعلوماتية، نظرا لشيوع استعمال تقنية المعلوماتية على مستواها بحكم التقدم التكنولوجي الذي أحرزته هذه الدول.

أولا : بالنسبة لنظام المملكة البريطانية المتحدة: أمام تحديات الجريمة المعلوماتية وقواعد نظام الإثبات المقيد ، اِهتدت المملكة المتحدة إلى حل لمواجهة الجريمة المعلوماتية من خلال الاعتراف بالدليل الإلكتروني كدليل إثبات جنائي بالرغم من تعارضه مع مبدئي استبعاد سماع الشهادة و الدليل الأصلي ، فبصدور قانون البوليس والإثبات الجنائي لسنة 1994، تم تحديد المسائل التنظيمية لقبول الدليل الإلكتروني في الإثبات الجنائي كإستثناء من قاعدة استبعاد سماع الشهادة . [1]

وإذا كان المشرع الإنجليزي قد قبل الدليل الإلكتروني في مجال الإثبات الجنائي على أساس أنه إستثناء من قاعدة استبعاد سماع الشهادة ، فإن الفقه اعتبره شهادة مباشرة وذلك حسب ما تم تداوله بشأن قضية (RV Wood) الذي عثر بحوزته على بعض المعادن الثمينة ، التي سرقت من قبل وقد كانت تركيبة هذه المواد مخزنة على حاسوبه ، وقد قدمت ورقة مخرجة من حاسوبه كدليل ، والسؤال الذي طرح بشأن ذلك هو هل تعتبر هذه الورقة الناتجة عن الحاسوب دليلا سماعيا وبالتالي لا يأخذ بها ؟

---

[1] – علي حسن أحمد الطوالبة–" مشروعية الدليل الإلكتروني المستمد من التفتيش"– مرجع سابق– ص 12.

أجابت المحكمة في هذا الشأن بالقول بأنها ورقة مقبولة وفقا للشريعة العامة وتصلح للإثبات وهي ليست من قبيل الشهادة السماعية ، وهو نفس الحكم الصادر عن محكمة الاستئناف في إنجلترا بقبول الدليل المستخرج من الحاسوب بمناسبة نظر قضية (pettig rew) والتي تضمنت قبول الدليل المخرج من حاسوب المتهم المتضمن الأرقام التسلسلية للأوراق النقدية التي قام بسرقتها وتسجيل أرقامها وتخزينها على حاسوبه.[1]

ثانيا : في نظام الولايات المتحدة الأمريكية : تناولت بعض القوانين في الولايات المتحدة الأمريكية حجية الأدلة الإلكترونية ، كما يتضح من قانون الإثبات الصادر سنة 1983 في ولاية كاليفورنيا أن النسخ المستخرجة من البيانات التي يحتويها الحاسوب تكون مقبولة بوصفها أفضل الأدلة المتاحة لإثبات هذه البيانات وكذلك ما نص عليه قانون الحاسوب الصادر سنة 1984 الصادر في ولاية (أيوا) والذي تبنى مبدأ أن مخرجات الحاسوب تكون مقبولة بوصفها أدلة إثبات بالنسبة للبرنامج والبيانات المخزنة فيه (المادة 716- أ- 16) .[2]

ويعتبر التشريع الأمريكي الأفضل من حيث تكييفه مع مبادئ الإثبات الجنائي الخاصة بالأدلة الإلكترونية، وهو ما تأكد من خلال تطوير وتعديل قانون الإثبات الفيدرالي الأمريكي، والذي مس نص (المادة 101. 1) التي أصبحت تشمل بمفهومها الدليل الإلكتروني بشكل موسع ، حيث سمحت بالإِعتراف بالمواد المكتوبة والمسجلة والإلكترونية ، لكي تحظى بذات الإِهتمام الذي تحظى به الأدلة الأخرى في المحاكم ، لذلك تم اعتبار الكتابة الموجودة في الحاسوب في صورة كهرومغناطيسية من قبيل النسخة الأصلية وبالتالي لا تصطدم بقاعدة الدليل الأصلي أو الأفضل، وبالتالي فالدليل الإلكتروني دليل أصلي.[3]

---

[1] - عائشة بن قارة- مرجع سابق - ص 204،203 .
[2] - علي حسن أحمد الطوالبة- التفتيش الجنائي على نظم الحاسوب والأنترنت - دراسة مقارنة- مرجع سابق -ص 198.
[3] - عائشة بن قارة- مرجع سابق- ص 206 - 207.

الفرع الثالث : موقف المشرع الجزائري من مسألة قبول الدليل الإلكتروني في مجال الإثبات الجنائي.

تنتمي الجزائر إلى مجموعة الدول التي تتبنّى نظام الإثبات الحر في مجال الإثبات الجنائي، فهي تساير النظم اللاّتينية كفرنسا وبلجيكا والأردن وسوريا في هذا المجال، وهو الأمر الذي كرسته (المادة 212 من قانون الإجراءات الجزائية)التي جاء في نصها على أنه" يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لإقتناعه الخاص، ولا يجوز للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه" ، إن فتح المشرع الجزائري باب الحرية في وجه تقديم الأدلة، وتركها لمعيار القناعة الشخصية لقاضي الموضوع هو تعزيز لمبادئ إثبات قرنية البراءة ، وتعزيز لمجال ممارسة حقوق الدفاع الفردية ، غير أن هذا الإطلاق بدون تحديد وتخصيص يعد قصورا تشريعا واضحا فلا نجد ضمن قانون الإجراءات الجزائية ما يدل على أن الدليل الإلكتروني هو دليل من نوع خاص شأنه شأن الجرائم المعلوماتية، فغياب أدنى نص قانوني في هذا الشأن من نتائجه أن تثار إشكالات متعلقة بطبيعة الأدلة المقدمة أمام الجهات القضائية، بحيث يمكن لهذه الأخيرة وفي حال عدم إلمامها بتقنيات المعلوماتية دحض هذا الدليل وعدم الإعتداد به، ولو كان حائزا على القوة الثبوتية، وتتوفر فيه كافة شروط الصحة وكذلك العكس صحيح، فلا حبذ لو اجتهد المشرع ووضع نصوصا خاصة تضبط أحكام الدليل الإلكتروني، كما فعل في نصوص القانون المدني الذي اعترف وبموجبه للتوقيع الإلكتروني بحجية كاملة في إثبات صحة العقد وذلك حسب نص (المادة 323 مكرر 01 . قانون 05 . 10 .) من القانون المدني الجزائري، فالأمر وبالنسبة للقانون الجنائي أشد وقعا على المتهم لأنه يتعلق بحريته وقرنية براءته اللتان تبقيان محل شك ونزاع وريبة في مواجهة الدليل الإلكتروني .

المطلب الثالث: معوقات البحث والتحقيق المعلوماتي .

تواجه مسألة البحث والتحقيق في مجال الجريمة المعلوماتية عدة عقبات تؤثر على فعاليتها بشكل مباشر، فالمسؤولية الملقاة على عاتق سلطات البحث والتحقيق من أجل التوصل لمرتكب الجريمة المعلوماتية عظيمة الشأن، وذلك راجع إلى الكيفية التي سيتم اكتشاف الجاني بها، والوسائل المتبعة في اللحاق به وتعقبه لأجل إثبات التهمة في حقه، وقد اتجهت أغلب الدول لاستخدام تقنية الحاسوب في تعقب المجرمين المعلوماتيين فقد أصبح هذا الاتجاه هو الأساس الأمني في أغلب الدول للكشف عن المجرم المعلوماتي.[1]

غير أن أمر في البحث والتحقيق المتعلق بالجرائم المعلوماتية وملاحقة مرتكبيها مهما اعتمد من وسائل حديثة فإنه يصطدم بالعديد من المعوقات التي يمكن لها أن تعرقل عملية التحقيق ، بل قد يؤدي بها إلى الخروج بنتائج سلبية تنعكس على نفسية المحقق من خلال فقدانه الثقة في نفسه، وعلى المجتمع بفقدانه الثقة في أجهزة تنفيذ القانون غير القادرة على حمايته من هذه الجرائم ، كما تنعكس على نفسية المجرم حيث يشعر أن الجهات الأمنية غير قادرة على اكتشاف أمره وأن خبرة القائمين على أمر البحث والتحقيق ومكافحة الجرائم المعلوماتية لا تجاري خبرته وعلمه، وهو ما يعطيه ثقة في النفس وتشجيعا على ارتكاب جرائم أخرى قد تكون أشد خطورة وقباحة.[2]

. وعليه فسنتناول بالدراسة في هذا المطلب أهم العقبات التي من شأنها أن تشكل عائقا في مواجهة إجراءات البحث والتحقيق المعلوماتي والتي يمكن تصنيفها على ثلاث (03) مستويات رئيسية هي :

- المستوى الأول متعلق بصعوبات مرّدها عمل جهة التحقيق (الفرع الأول).

---

[1] – ناير نبيل عمر – مرجع سابق – ص 162 .

[2] – علي عدنان الفيل – مرجع سابق- ص 79.

- المستوى الثاني متعلق بصعوبات مرّدها طبيعة الجريمة (الفرع الثاني).
- المستوى الثالث متعلق بصعوبات مرّدها الضحية في جرائم المعلوماتية (الفرع الثالث).

الفرع الأول :الصعوبات المتعلقة بعمل جهة البحث والتحقيق.

إن التعرض إلى جملة الصعوبات التي تواجه عمل جهة البحث والتحقيق تقودنا إلى الحديث عن نوعين من الصعوبات أولها : جملة المعوقات أو الصعوبات التشريعية ، وثانيها : صعوبات راجعة إلى الكادر البشري المكون لجهة البحث والتحقيق ومدى كفاءته في التعامل مع هذا النوع من الجرائم وقدرته على استخلاص الأدلة الإلكترونية .

الفقرة الأولى : المعوقات التشريعية .

تنحصر هذه المعوقات أو الصعوبات في قصور النصوص التشريعية الخاصة بمكافحة الجريمة المعلوماتية وكذلك الإجرائية منها والخاصة بالبحث والتحقيق في الجرائم المعلوماتية وذلك على مستويين.

أولا : على مستوى التشريعات الداخلية : يؤدي عدم وجود نص التجريم الخاص بالظاهرة الإجرامية المعلوماتية إلى تفاقم هذا النوع من الجرائم، وبلوغه مرحلة يصبح فيها أمر علاج هذه الظاهرة أصعب مما قد يتوقع خصوصا أن جميع المعاملات والإجراءات تسير نحو التحول إلى الطابع الإلكتروني ، فنجد أن القضاء لا يعتمد الأدلة والقرائن التي تعدها هيئات الضبط والتحقيق في الجرائم المعلوماتية ، وذلك راجع أساسا إلى غياب القوانين والعقوبات الملائمة لطبيعة الجرائم المعلوماتية. [1]

1- من خلال استقراء نصوص المواد 394 مكرر في قانون العقوبات الجزائري نجد أن التشريع الجزائري لم يتعامل بالجدية اللاّزمة من الناحية القانونية مع خطورة هذه الجرائم وذلك من خلال جموده منذ سنة 2004 والذي اعتمد أسلوب التشريع المتسرع في التعامل مع هذه الجرائم التي تحتاج إلى تجديد دائم لمفاهيمها وصورها وتكيف عقوباتها بالشكل الملائم .

إضافة إلى ذلك فإننا نجد وعلى مستوى الإجرائي لقانون الإجراءات الجزئية قصورا تشريعيا يتمثل في غياب النصوص القانونية الملاّئمة لمواجهة الطبيعة الخاصة للجرائم المعلوماتية وذلك على النحو التالي :

1- عدم وجود قواعد خاصة تنظم التفتيش على الحاسوب عندما يكون هذا الأخير متصلا بآخر خارج إقليم الدولة .

2 - عدم ملائمة نظرية الإثبات الجنائي وخصوصيات الدليل الإلكتروني .

3- عدم وجود نصوص تسمح بمواجهة رفض المتهم إعطاء الرقم السرّي للدخول إلى حاسوبه لأجل التفتيش وبالتالي تمتعه بفرصة تدمير الأدلة .

4- عدم وجود نصوص خاصة تحدد قواعد الإختصاص الإقليمي في مواجهة الجريمة المعلوماتية، وهو ما يخلق صعوبة تتعلق بالإختصاص المكاني فيمكن أن تكون الأدلة الجرمية خارج نطاق سلطة التحقيق أي خارج صلاحيتها القانونية ، وبالتالي لا تستطيع ممارسة أي إجراء إلا عن طريق طلب الإعانة الدولية وهو ما يؤدي إلى إفلات المتهم من العقاب نظرا لطول إجراءات التحقيق وتعقيداتها وهو ما يتيح له فرصة محو الدليل.[1]

ثانيا: غياب التنسيق التشريعي على المستوى الدولي : من خصائص جرائم الحاسوب أنها جرائم عابرة للحدود الوطنية فهي ذات طابع دولي ،وهو ما يتطلب العمل بشكل مؤثر على إنماء العمل الدولي المشترك لمواجهة هذه الظاهرة وذلك من خلال وضع حلول للمشاكل التي تحد من فاعلية مكافحتها سواء المشاكل الناجمة عن تطبيق القواعد الموضوعية أو الإجرائية وأهم العقابات التي تقف بمثابة حجر عثرة في مجال مكافحة الجرائم المعلوماتية عموما وأعمال البحث والتحقيق خصوصا هي:

---

[1] - خالد عياد الحلبي - مرجع سابق - ص 220، 221 .

1- عدم وجود مفهوم مشترك بين الدول حول نماذج الجريمة المعلوماتية .

2- عدم وجود تعريف قانوني موحد بين الدول حول نماذج الجريمة المعلوماتية .

3- اختلاف مفهوم الجريمة المعلوماتية لِإختلاف التقاليد القانونية وفلسفة النظم القانونية .

4- انعدام التنسيق بين قوانين الإجراءات الجنائية للدول فيما يتعلق بأعمال البحث والتحقيق .

5- تعقد المشاكل القانونية والفنية خاصة المتعلقة بتفتيش نظم المعلومات خارج حدود الدولة ومسائل ضبط الأدلة الإلكترونية وتسليمها.

6- قلة المعاهدات الخاصة بمسائل التسليم والتعاون بين الدول في مجال مكافحة الجريمة المعلوماتية وحتى وإن وجدت فهي غير كافية لمواجهة الظاهرة.

7- ضعف وسائل أغلب دول العالم الثالث في مواجهة الظاهرة الإجرامية المعلوماتية وتأثير ذلك على جهود الدول الأخرى، فتشكل هذه الدول ملجأ آمنا لمجرمي المعلوماتية نظرا لغياب النصوص العقابية أو من خلال نظمها المعلوماتية التي تفتقر إلى الحماية الأمنية المعلوماتية.[1]

الفقرة الثانية: الصعوبات المتعلقة بمدى فعالية جهات البحث والتحقيق.

أولا : قلة خبرة القائمين على البحث والتحقيق بمجال المعلوماتية : من الصعوبات التي تواجه عملية استخلاص الدليل في الجرائم المعلوماتية، هو نقص الخبرة لدى رجال البحث والتحقيق، وأجهزة الأمن بصفة عامة، وكذلك لدى أجهزة العدالة الجنائية ممثلة في سلطة الاِتهام والتحقيق والمحاكمة، إن النقص يسجل خصوصا على مستوى الثقافة المتعلقة بالأنظمة المعلوماتية وكيفيات التعامل مع الحواسيب، إضافة إلى عدم الإلمام بعناصر الجرائم المعلوماتية، وتقنية مجرمي المعلوماتية، وهي العوائق التي تؤثر

1- عبد العال الدريبي – مرجع سابق – ص 342 .

سلبا على عمليات البحث والتحقيق ومكافحة الجريمة المعلوماتية، وذلك في البلدان العربية خصوصا، نظرا لتأخرها في مجال التقنية المعلوماتية مقارنة بالدول الأوروبية والولايات المتحدة الأمريكية، فمسألة مكافحة هذا النوع من الجرائم والتعامل معها على المستوى الإجرائي، يعتمد على التكوين عقب ظهور هذه الجرائم، وهو ما يستغرق وقتا يجعل من سرعة انتشار هذه الجرائم موازية لسرعة اِنتشار التقنيات الحديثة للمعلوماتية، ويخلق فرقا شاسعا بين الحركية التشريعية والثقافة الأمنية والقانونية لجهات البحث والتحقيق وهذه الجرائم ، فهما لا يسيران بنفس معدل السرعة، وهو الفارق في التقدم والتطور الذي ينعكس سلبا على إجراءات البحث والتحقيق في الجرائم المعلوماتية الذي يظهر جليا في عدم تأهيل سلطات وجهات التحقيق في هذه الجرائم.[1]

ثانيا: نقص ثقافة سلطات البحث والتحقيق في مجال المعلوماتية : يتطلب أمر الكشف عن الجرائم المعلوماتية والوصول إلى مرتكبها، استراتيجيات خاصة تتعلق أساسا باستعمال مهارات خاصة من قبل رجال سلطة البحث والتحقيق على نحو يساعدهم على مواجهة التقنيات الإجرامية الحديثة، لذا يجب استخدام تقنيات مناسبة ومبتكرة لتحديد نوعية الجريمة المرتكبة، وشخصية فاعلها وأسلوبه ، مع الاِستعانة بوسائل حديثة لجمع الدليل الإلكتروني، فمن المتصور أن يجد رجال البحث والتحقيق أنفسهم غير قادرين على التعامل بالوسائل الاِستدلالية التقليدية مع هذا النوع من الجرائم. [2]

لقد اِهتمت أجهزة الأمن في الكثير من الدول في مجال مواجهة جرائم المعلوماتية بإنشاء وحدات خاصة بمكافحة جرائم المعلوماتية ، كما سبق وأن فصلنا ذلك في المبحث الثاني من الفصل الثاني

1- عبد الفتاح بيومي حجازي- الدليل الجنائي في جرائم الكمبيوتر و التزوير- دراسة معمقة في جرائم الحاسب الآلي والأنترنت- دار الكتب القانونية- مصر- 2004- ص 81 .

[2] - عبد العال الدريبي - مرجع سابق - ص 336 .

لموضوع بحثنا، وتعتبر الولايات المتحدة الأمريكية و فرنسا من الدول الرائدة في هذا المجال، نظرا لمعاناتها بشكل كبير من الجرائم المعلوماتية، وهو ما دفعها لإنشاء وحدة متخصصة للمكافحة والتحقيق في الإجرام المعلوماتي على طراز تلك التابعة لمكتب التحقيقات الفيدرالي الأمريكي (FBI).[1]

وتواجه الأجهزة الأمنية خطر الفشل في مهامها نظرا لسوء تقديرها لأهمية الجريمة محل البحث والتحقيق، وذلك لقلة خبرتها وتدريبها وهو ما يجعلها تفشل في جمع الدليل ، فالمحقق أحيانا يكون السبب في تدمير الدليل الإلكتروني خطأ منه أو إهمالاً، أو بسبب تسرعه في التعامل مع الأدلة، ويمكن أيضا له أن يكون سببا في ذلك في حال:

- تجاهل الدليل تماما.
- محاولة فحص الدليل دون اِتباع المهارات اللاّزمة في مجال المعلوماتية.
- حمل المشبه فيه على اِستعادة معلومات من الحاسوب، بسبب عدم معرفة ذلك، مما يسمح للمشبه فيه بتدمير الدليل ومحوه تحت أنظار المحقق.
- مصادرة وحجز أجهزة الحاسوب دون أدنى تعامل تقني معها وهو ما يزيد من فرضيات فقد الأدلة.[2]

ثالثا : صعوبات متعلقة بضعف الوسائل المادية : إن التحقيق في مجال الجرائم المعلوماتية يحتاج إلى خبرات ومختصين في المجال، وهؤلاء يحتاجون وبصفة دورية ومستمرة إلى دورات تكوينية وتدريبية، لأجل تحسين معارفهم وتطور التقنية المعلوماتية ، وهو الأمر الذي يتطلب تكاليف باهظة.[3]

---

[1] – خالد عياد الحلبي – مرجع سابق – ص 225 .

[2] – عبد العال الدريبي – مرجع سابق – ص 337، 338 .

[3] – خالد عياد الحلبي – مرجع سابق – ص 228 .

فالميزانية المالية الخاصة بأجهزة الأمن والقضاء تكون ضعيفة في مجال تغطية احتياجات خبراء الحاسوب ، فضلا على أنها لا تصل إلى ذات المبالغ التي تسددها المؤسسات الخاصة.[1]

وحسب الدراسة التي قام بها الباحث عبد الله بن سعود بن محمد السراني في إطار عملية البحث تحت عنوان فعالية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني سنة 2009 حول عينة مفردات بحث لأجل تحديد المعوقات التي تؤدي إلى عدم فعالية الأساليب المستخدمة من قبل المحقق الجنائي في مجال إثبات الجرائم المعلوماتية في المملكة العربية السعودية فإنه جاء وعلى رأس ترتيب الأسباب :

- ندرة البرامج التدريبية اللاّزمة لتأهيل المحققين بحيث وافق على ترتيب هذا السبب في المقام الأول 99,5 % من أفراد عينة البحث ، بينما جاء معوق قلة الإمكانات الفنية اللاّزمة لإثبات الجرائم المعلوماتية في المركز الرابع من حيث الأهمية بمعدل موافقة بلغ 97,9 % من أفراد عينة البحث.[2]

إضافة للأسباب السالفة الذكر توجد أسباب أخرى تؤثر على عمل جهات البحث والتحقيق في مجال الجريمة المعلوماتية يمكن إيجازها في النقاط التالية :

- عدم الإهتمام الكافي بالجريمة المعلوماتية من قبل الأجهزة الأمنية وانشغالها بالجرائم التقليدية.
- الإنتشار المتزايد لتقنية المعلوماتية في الأوساط الإجتماعية خصوصا ، وتحولها إلى تقنية محمولة ومتنقلة نظرا لانتشار تقنية خدمة الاتصال بالأنترنت عبر الهواتف الذكية المزودة بتقنية الجيل الثالث ، وعدم تكييف الأجهزة الأمنية بعد من هذه التقنيات الحديثة .

---

[1] – حجازي عبد الفتاح بيومي – الدليل الجنائي في جرائم الكمبيوتر و التزوير– دراسة معمقة في جرائم الحاسب الآلي والأنترنت – مرجع سابق – ص 84 .

[2] – عبد الله بن سعود بن محمد السراني – مرجع سابق – ص 196 .

إذن فمعوقات التحقيق ومن ناحية جهة التحقيق عديدة ومتنوعة ، ومؤثرة بشكل سلبي على عمل هذه الجهة وعلى مسألة مكافحة الجريمة المعلوماتية ، وهو ما يستدعي وعلى سبيل الاستعجال وضع استراتيجيات فعالة تضمن التكوين المستمر لرجال الضبط والقضاء في مجال الجرائم المعلوماتية بشكل سمح لهم بمواكبة معدل سرعة انتشار وتطور هذا النوع من الجرائم .

الفرع الثاني : صعوبات متعلقة بطبيعة الجرائم المعلوماتية وآثارها.

تشكل الجريمة المعلوماتية في حد ذاتها عائقا حقيقيا أمام عمل جهات البحث والتحقيق، بالنظر إلى طبيعتها، والتي تجعل من أمر إثباتها أمرا غاية في الصعوبة حتى وفي حال توفر عامل الخبرة البشرية وتوفر الوسائل المادية الملائمة، ويمكن حصر هذه الصعوبات في النقاط التالية:

الفقرة الأولى : صعوبات تفرضها الجريمة المعلوماتية في حد ذاتها .

تقع الجريمة المعلوماتية على الحواسيب وشبكات الاتصال أو بواسطتها، وأهم ما يميزها هو أنها جرائم خفية غير مرئية ، لا يلاحظها المجني عليه ، بل لا يدري حتى بوقوعها ، فليس من العسير على المجرم المعلوماتي حجب وإخفاء السلوك المكون لهذه الجرائم وطمس نتائجها ، عن طريق التلاعب غير المرئي بالنبضات والذبذبات الإلكترونية التي تسجل البيانات عن طريقها ، بحكم خبرته في مجال الحواسيب .[1]

ونتيجة لهذه الصعوبة أصبح لإمكانية إخفاء الجريمة المعلوماتية عن طريق التلاعب بالبيانات مصطلح خاص يستعمل في أبحاث علم الإجرام الأمريكي وهو الطبيعة غير الأولية لمخرجات الحاسوب المطبوعة (SNCP) (Second naud Nature Computer print outs) .[2]

---

[1] – ضياء علي أحمد النعمان – مرجع سابق – ص 341 .

[2] – عبد العال الدريبي – مرجع سابق .–ص 326 .

و لعل ان الإشكاليات ستتعاظم و تزداد تعقيدا في مجال البحث و التحقيق المعلوماتي ، و ذلك بسبب إستحداث مجرمي المعلوماتية أسلوب التخفي عبر الشبكة من خلال إستعمالهم لوسيلة مستحدثة في مجال التواصل عبر الشبكات و هي ما يعرف بـ " الشبكة الخفية للنت " أو ما يصطلح عليه باللغة الإنجليزية و في لغة المعلوماتية " The Darknet" ، و هي شبكة موازية لشبكة الأنترنت العادية ، و قد ظهرت للوجود أول مرة سنة 1970 في الولايات المتحدة الأمريكية ، لأجل تأمين المعلومات العسكرية المتنقلة عبر شبكة " ARPANET" ، ثم دخلت عالم المعلوماتية سنة 2002 ، و يكفي لولوج الشبكة الخفية و الإبحار عبرها تحميل تطبيق معلوماتي متوفر على شبكة الأنترنت ، و تفعيله على جهاز الحاسوب ، و لعل أن أشهره هو تطبيق " TOR" "The Onion Router" ، يعمل على هذا الأخير على تغيير العنوان الإلكتروني للحاسوب " IP" المتصل بالشبكة الموازية الخفية عدة مرات في الساعة الواحدة ، فإذا كان المستعمل متصلا من فرنسا حقيقة فإنه يظهر متصلا تارة من الولايات المتحدة الأمريكية و تارة من اليابان و تارة من إنكلترا و هكذا علة مدار مدة الإتصال بالشبكة ، و هو ما يجعل من امر إقتفاء أثر المجرم المعلوماتي غاية في التعقيد إن لم يكن مستحيلا .[1]

الفقرة الثانية: صعوبات ناجمة عن طبيعة آثار الجريمة المعلوماتية.

ينتج عن الجريمة المعلوماتية آثار من نوع خاص تعرف بالدليل الإلكتروني ، كما سبق وأن فصلنا في تعريفه وبيان خصائصه في المطلب الأول من هذا البحث ، ولخصائص هذا الدليل آثار سلبية على

---

[1] – William Gilles et Jean Harivel et Iréne Bouhadana –« Darknet le coté obscur du net »– Article publier sur : Panthéon Sorbonne Magazine – Magazine D'information de L'université Paris 1 Panthéon Sorbonne – Num 06– Janvier – Février – 2014– Paris – France .

عمل جهات البحث والتحقيق بحيث تعيق عملهم في مجال إحراز هذا الدليل وهي الصعوبات التي سنوجزها في النقاط التالية :

أولا : غياب المظهر المادي عن الدليل الإلكتروني : الدليل الإلكتروني عبارة عن سجل كهرومغناطيسي مخزن في نظام حاسوبي بشكل ثنائي ، وبطريقة غير منظمة ، فعلى سبيل المثال فإن الأقراص الصلبة تتضمن مزيجا بين البيانات المختلطة فيما بينها، أي أنها خليط بين الملفات البريئة وتلك المجرمة موضوع الدليل ، وهو ما قد يخلف مشكلة التعدي على الخصوصية ، إذن فالدليل المرئي مختلف عن الإلكتروني ، وبالتالي فإن أمر ربطه بشخصية المتهم أمر بالغ في الصعوبة ، فالدليل الإلكتروني لا يفصح عن شخصية معينة ، وهو ما يظهر جليا في الجرائم المرتبكة عبر الشبكة والتي يستطيع المستخدم عبرها الإتصال دون الكشف عن هويته الحقيقية إضافة إلى كون الدليل الرقمي عادة مشفرا ، إضافة إلى إمكانية تعديله والتلاعب به عن بعد مما قد يقطع علاقة السببية بين المجرم والجريمة. [1]

ثانيا : سهولة محو الدليل وتدميره : من المعوقات التي تقف وجه إتمام عمليات التحقيق المعلوماتي، سهولة محو الدليل الإلكتروني وتدميره وذلك في زمن قصير فالجاني يمكنه محو الأدلة التي تكون قائمة ضده أو تعديلها في زمن قصير جدا بحيث لا تتمكن السلطات من كشف الجريمة إذا علمت بها. [2]

ثالثا : صعوبة الوصول إلى الدليل الإلكتروني : عادة ما تحاط البيانات المخزنة إلكترونيا أو المتنقلة عبر الشبكة بجدار من الحماية الفنية لإعاقة محاولة الوصول غير المشروع إليها ، للإطلاع عليها أو استنساخها ، فيمكن للمجرم المعلوماتي أن يزيد من صعوبة عملية التفتيش التي قد تباشر للحصول على الأدلة التي تدينه، عن طريق مجموعة من التدابير الأمنية كاستخدام كلمات السر ، أو دسّ تعليمات خفية

---

[1] – عائشة بن قارة – مرجع سابق – ص 251 – 252 .

2– خالد عياد الحلبي – مرجع سابق – ص 223 .

أو ترميزها لمنع الإطلاع عليها ، ولعل أن الإشكال يتفاقم في حال تخزين هذه المعلومات خارج حدود الدولة بحيث تصطدم عملية الوصول إلى الدليل الإلكتروني بمشكلة إجرائية تتعلق بمدى سريان النصوص الإجرائية من حيث المكان على هذه البيانات .[1]

رابعا: مشكلة الأصالة في الدليل الإلكتروني : إن الأصالة في الدليل الإلكتروني لها طابع افتراضي لا يرتقي إلى مستوى الأصالة بالنسبة للدليل المادي فهذه الأخيرة تعبير عن وضع مادي ملموس، في حين أن الدليل الرقمي عبارة عن تعداد غير محدود من أرقام ثنائية موحدة في الصفر والواحد (0 . 1) فكل شيء في العالم الرقمي يتكون من الصفر والواحد (0 . 1) ، وهما عبارة عن نبضات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة ، وقد أثارت مسألة الأصالة في الدليل الإلكتروني إشكالية مدى قبولها في مجال الإثبات الجنائي على اِعتبار اِفتقادها للمظهر المادي الملموس .[2]

إذن فالجريمة المعلوماتية بحكم طبيعتها وآثارها تشكل عائقا لسير الإجراءات الخاصة بالبحث والتحري في شأن ذلك ، فالجريمة المعلوماتية جريمة دائمة التطور وهو ما يخلق مع كل تطور نوعا جديدا من الأدلة الإلكترونية لم تكن معروفة مسبقا ولم يتم التعامل معها قبلا وهو ما يشكل فرصة للجاني للإفلات من العقاب ، إضافة لكل ذلك هناك نوع آخر من الصعوبات والعوائق التي تعرقل سير إجراءات التحقيق مرّدها الضحية في حدّ ذاته ، فما هي يا ترى هذه العوائق ؟

---

[1] – عبد العال الدريبي – مرجع سابق – ص 329 – 330.

[2] – عائشة بن قارة – مرجع سابق – ص 252

الفرع الثالث: صعوبات متعلقة بالإحجام عن التبليغ .

تظل الجريمة المعلوماتية مستمرة ما لم يتم الإبلاغ عنها، ومن ثم فإنه لا يمكن اِتخاذ أي إجراء من أجل تحريك الدعوى الجنائية، فالصعوبة التي تواجه أجهزة الأمن والمحققين هي أن هذه الجرائم لا تصل إلى علمهم بالصورة العادية كما هو عليه الحال في الجرائم العادية ، وذلك لصعوبة اكتشافها من قبل الضحايا.[1]

ويُعبر عن الجرائم غير المبلغ عنها بمصطلح " الرقم الأسود " لجرائم المعلوماتية ، ففي هذا الشأن يحدثنا Beter Swift عضو اِتحاد الصناعة البريطاني أن العديد من الشركات تقع في حرج من الاِعتراف بأنها تعرضت للسلب من قبل مجرمي المعلوماتية ، فبدلا من اِستدعاء الشرطة والتبليغ فإنهم يخلدون إلى الصمت ، إن العديد من الضحايا في جرائم المعلوماتية لا يقفون عند حد عدم الإبلاغ عن الجريمة ، بل أنهم يرفضون أي تعاون مع الجهات الأمنية خشية معرفة العامة بوقوع الجريمة ، ويسعون بدلا من ذلك إلى محاولة تجاوز آثارها حتى لو كانت الوسيلة هي مكافأة المجرم ونذكر على سبيل المثال ما قام به بنك Marchant Bank City الإنجليزي الذي تعرض لسرقة 08 مليون جنيه أثناء تحويلها إلكترونيا إلى رصيد في سويسرا ، وقد تم القبض على الفاعل أثناء محاولة سحبه المبلغ ، وبدل رفع البنك دعوى ضد المتهم قام مسؤول البنك بدفع مبلغ 01 مليون جنيه مقابل شراء سكوته وعدم إبلاغه الغير طريقة القيام بذلك مع إعلامهم بالثغرة التي سمحت له القيام بذلك .[2]

---

[1] – عبد العال الدريبي – مرجع سابق – ص 339 .

1– عبد الفتاح بيومي حجازي – الدليل الجنائي في جرائم الكمبيوتر و التزوير– دراسة معمقة في جرائم الحاسب الآلي والأنترنت – مرجع سابق – ص 68 .

وقد أكدت بعض الدراسات في هذا المجال كتلك الذي قام بها المعهد الوطني للعدالة التابع لوزارة العدل الأمريكية والتي شملت 128 من العاملين في مجال التحقيق الجنائي المعلوماتي والذين يمثلون 114 وكالة رسمية ، بأن غالبيتهم أكدوا أن معظم جرائم المعلوماتية التي يتم اكتشافها لا يتم التبليغ عنها للشرطة، وهو ما أكدته دراسة معهد CSI بالاِشتراك مع مكتب التحقيقات الفيدرالي FBI فإن حوالي 70 % من الجرائم المعلوماتية المكتشفة لا يتم التبليغ عنها.[1]

ويمكن إيجاز الأسباب الرئيسية للإحجام عن الإبلاغ فيما يلي :

- عدم إدراك خطورة الجرائم المعلوماتية من قبل المسؤولين على المؤسسات وكذلك من قبل الأفراد وجهلهم بأنها جرائم معاقب عليها قانونا .
- خوف الجهات المتضررة من الجريمة وخاصة الشركات والمؤسسات المالية من انتشار خبر تعرضها للاِعتداء، مما قد يترك أثرا على سمعتها ومصداقيتها ، مما قد يوحي بإهمالها وقلة خبرتها وعدم وعيها الأمني، وهو ما قد ينعكس سلبا على أرباحها وقيمة أسهمها.
- خوف الشركات والمؤسسات من أن تؤدي أعمال التحقيق إلى احتجاز نظمها المعلوماتية وتعطيل شبكات عملها لمدة طويلة مما يسبب لها خسائر مالية ، و اِنعدام الثقة لدى بعض الضحايا في جهات إنفاذ القانون حول مدى قدرتها على التعامل مع هذه الجرائم.[2]
- خوف الضحايا من انتشار الأساليب الإجرامية المعلوماتية مستقبلا .
- محدودية آثار الجريمة المعلوماتية على وقع الضحايا مما يدفعهم لعدم الإبلاغ .

---

[1] – حسين بن سعيد الغافري – مرجع سابق – ص 19 – 20.

2– علي عدنان الفيل – مرجع سابق – ص 83 .

- خوف الموظفين وفي حال الإبلاغ عن الجرائم المعلوماتية من اتخاذ الجهة المسؤولة عن تشغيل النظام المعلوماتي من حرمانهم من خدمة الأنترنت أو تحديد قائمة المواقع التي يسمح لهم بزيارتها .[1]

تشكل جل هذه الأسباب الدوافع الرئيسية التي تمنع الضحايا في حال الإجرام المعلوماتي من الإبلاغ عن الاعتداءات الإلكترونية ، وقد اجتهد الفقه في وضع مجموعة من التوصيات من أجل الحد من تضخم الرقم الأسود للجريمة المعلوماتية ، وهي مجموعة من التدابير الواجب تطبيقها على أرض الواقع ، غير أن ذلك مرتبط بقدرات الجهات الأمنية ومدى كفائتها في رصد هذه الجرائم إضافة إلى مدى الوعي العام للمواطنين وهذه التدابير هي :

- تعليم رجال الأمن مبادئ العلوم الحاسوبية وكيفية التعامل معها .
- تخصيص وحدات أمنية تعد بمثابة شرطة متخصصة تكثف من تواجدها ونشاطها في رصد الإِعتداءات الإلكترونية على مستوى البنوك والمؤسسات التجارية والمالية ومصالح البريد والهاتف، إضافة إلى مراكز بنوك المعلومات والمصالح العمومية ، كمصالح العدالة والقضاء إضافة إلى التواجد الميداني على مستوى أسواق أجهزة الحاسوب والبرمجيات باعتبارها ملتقى مجرمي المعلوماتية.[2]

إذن فما يمكن استخلاصه من هذا المبحث أن نتائج البحث والتحقيق المعلوماتي هي نتائج من نوع وطبيعة خاصة تتمثل في الدليل الإلكتروني ، هذا الأخير الفريد من حيث نوعه وطبيعته الرقمية ، والذي يفتقر للمظهر المادي ، والذي كسب الاعتراف القانوني بمدى قوته الثبوتية في مجال الإثبات الجنائي ، تحت وطأة تنامي الظاهرة الإجرامية المعلوماتية فالدليل الإلكتروني يعتبر الدليل الأنسب

---

[1] – حسين بن سعيد الغافري – مرجع سابق – ص 20.

2– عبد الفتاح بيومي حجازي – الدليل الجنائي في جرائم الكمبيوتر و التزوير– دراسة معمقة في جرائم الحاسب الآلي والأنترنت – مرجع سابق – ص 72، 73 .

والمتلائم مع هذا النوع من الجرائم ولعل ما يجب الإشارة إليه أن التشريع الجزائري ومقارنة بما وصلت إليه التشريعات المقارنة الأوروبية خصوصا ، يعتبر تشريعا فتيا في بدايات الطريق في مجال مكافحة الجرائم المعلوماتية ، وذلك راجع إلى غياب التجديد في التشريع ، الذي يعتبر سلاح الجهات المختصة في مكافحة الجرائم المعلوماتية ، فمجرد التأخر في تجديد النصوص القانونية يجعل منها جامدة وغير فعالة في مواجهة الجرائم المعلوماتية ، إضافة إلى باقي العقبات الأخرى الناتجة عن طبيعة الجرائم المعلوماتية والأدلة الإلكترونية ، أو تلك المتعلقة بنفسية الضحايا ... إلخ ، وهي كلها عوامل سلبية تجعل من أمر البحث والتحقيق الجنائي المعلوماتي أشد صعوبة وتعقيدا مما هو عليه أصلا .

خلاصة الفصل .

كختام لفصلنا هذا كان لنا ان نلخص معطياته بالقول بأنه و في إطار تنفيذ الإجراءات الخاصة بمباشرة أعمال البحث و التحقيق في مجال الجرائم المعلوماتية ، و نظرا للطابع الخاص للجريمة و ما يصاحبها من أدلة و أثار ، فإن هذه المهمة عادة ما تُسند لوحدات خاصة تعمل على تولي زمام امور أعمال البحث و التحقيق من خلال تمتعها بمزايا الإختصاص القانوني و المعرفي العلمي بمجال المعلوماتية ، و هو ما يسمح لها بأداء مهامها على احسن وجه مراعاة للمصلحة العامة و حماية لحقوق الضحية ، و ذلك من خلال إتباعها لأساليب خاصة و تقييدها بنصوص إجرائية ذات طبيعة خاصة تمزج بين النصوص العامة و الخاصة لأجل ضمان أفضل توازن لمبدئي " حسن سير الإجراءات" و " حرية الأفراد"، إن عمل هذه الجهات يتميز بالدقة و الطابع الفني فهو عمل أساسه مبدأ الشرعية الإجرائية ، و هدفه تحصيل الدليل الذي يثبت براءة المتهم من إحتمال إدانته ، و أساس ذلك هو الدليل الإلكتروني ، أي ذلك الأثر الذي يتركه و يخلفه من بعده الجرم المعلوماتي ، إما على الشبكة أو على الحاسوب أو إحدى لواحقه ، و هو دليل و اثر جنائي من نوع خاص فهو معنوي يفتقد للمظهر المادي المحسوس ، لا يمكن لمسه و لا تحسسه كباقي الأدلة الجنائية الأخرى ، و كل ما في الأمر أنه لا يمكن تحصيله و لا إستعراضه إلا من خلال الإستعانة بوسائل إلكترونية و برامج خاصة ، و هي المهمة التي تتخللها و تقف في وجهها عدة عقبات تعيقها و تعرقل أعمال البحث و التحقيق المعلوماتي ، و هي و على إختلافها عوائق نابعة من الطبيعة الخاصة للجريمة المعلوماتية ، و التي تعتبر تحديا للواقع القانوني نظرا لما تشهده من سرعة في التطور المصاحبة لكل ما هو حديث في عالم المعلوماتية ، و لما يعانيه القانون من وتيرة بطيئة في مجال تطوره و مسايرته لتطور الأساليب الإجرامية في مجال المعلوماتية ، إضافة إلى عوائق متعلقة بضعف تكوين و تأهيل الجهات المكلفة بمباشرة أعمال البحث و التحقيق بمجال

المعلوماتية ، و كذلك عائق عدم التبليغ عن الجرائم من قبل الضحايا الذين عادة ما يتخذون موقفا سلبيا تجاه ما لحقهم من ضرر جراء الجريمة المعلوماتية ، جهلا منهم لحجم الخطر و الضرر او تسترا منهم على ذلك ، خوفا من ردة فعل الغير تجاههم ، و هي كلها عوائق تعيق أعمال البحث و التحقيق في الجرائم المعلوماتية .

و هذا ما يمكننا من إستخلاص مجموعة من النتائج و هي :

- لا يوجد مجال لإعمال الإجراءات الخاصة بالبحث و التحقيق في الجرائم التقليدية في مواجهة الجرائم المعلوماتية ، فهذه الأخيرة و نظرا لطبيعتها الخاصة تستلزم إجراءات من نوع خاص تتلائم و طبيعتها .
- يعتمد نجاح و ضمان فعالية الإجراءات الخاصة بالبحث و التحقيق في الجرائم المعلوماتية على عنصرين أساسين يكمل أحدهما الأخر و لا يمكن تصور نجاح هذه الإجراءات في الوصول إلى مبتغاها في غياب أحد هذين العنصرين و هما :

1. العنصر البشري المؤهل للقيام بمهام البحث و التحقيق في الجرائم المعلوماتية ، و الذي يجمع بين كفاءة البراعة في أعمال البحث و التحقيق القضائي ، و الخبرة و المعرفة الدقيقة بالمجال المعلوماتي و الأساليب الإجرامية المعلوماتية و نفسية الجناة.
2. العنصر المادي و المتمثل في الوسائل الخاصة بوضع الخطط المتعلقة بمتابعة الجرائم المعلوماتية حيز التطبيق ، كالبرامج الخاصة بالتتبع الإلكتروني و إقتفاء الأثر، و تحديد المواقع على الشبكة ......إلـــخ من و سائل مساعدة على إستعادة الأدلة الإلكترونية و حفظها.

- إستحداث مفهوم جديد في علم الأدلة الجنائية و هو " الدليل الإلكتروني " و ذلك كنتيجة حتمية لإنتشار الظاهرة الإجرامية المعلوماتية ، و تزايد حدتها و تهديداتها ، و هو ذلك العنصر الكفيل بإثبات براءة المتهم من إدانته في مواجهة التهم الموجهة إليه ، بشأن الجريمة المعلوماتية المنسوبة إليه ، و هو الدليل

الذي واجه عدة عقبات فرضها الفقه القديم و غياب النصوص التشريعية الملاءمة له ، من أجل أن يحوز على الإعتراف الفقهي و القانوني في مجال الإثبات الجنائي .

- مواجهة أعمال البحث و التحقيق الجنائيين في مجال الجرائم المعلوماتية لعقبات تمنع من إتمام إجراءات تحصيل الدليل الإلكتروني ، او تعيق ذلك بشكل يسمح لمرتكب الجريمة من تدمير الأدلة و الفرار من قبضة العدالة ، و اهم العقبات و العوائق في هذا الشأن هي :

1. عقبات ذات طابع تشريعي و التي يمكن تجاوزها من خلال وضع حلول مستعجلة .
2. عقبات تقنية راجعة لطبيعة الجريمة و لضعف الكادر البشري في مجال التعامل مع نطاق المعلوماتية، أو لقلة و إنعدام الوسائل المادية المستعملة في اعمال البحث و التحقيق، و هي عقبات يصعب حلها بصفة سريعة و مستعجلة نظرا لطول مدة تكوين و تدريب الكوادر البشرية في هذا المجال ، و كذلك الحال في مجال التعامل مع الوسائل المادية و البرمجية الحديثة الخاصة بمكافحة الجرائم المعلوماتية .
3. عقبات نفسية مردها ضحايا الإجرام المعلوماتي، و الذين يتسببون جراء قلة إدراكهم بحجم المخاطر التي تفرضها الجريمة المعلوماتية ، أو خوفهم من إنتشار أمر وقوعهم ضحايا الجريمة المعلوماتية ، من خلال إحجامهم عن التبليغ في تعطيل يد الجهات المختصة بالبحث و التحقيق عن أداء مهامها ، كما يعملون بذلك على تشجيع مجرمي المعلوماتية على التمادي في إجرامهم ظنا منهم بأنه لم يتم كشف أمرهم ، و هي من أصعب العقبات التي تواجه أعمال البحث و التحقيق في مجال الجرائم المعلوماتية ، بالنظر إلى صعوبة إقناع الغير بحجم الخطر الكامن وراء إحجامهم عن التبليغ ، و تفضيلهم التكتم عن أمر الجرائم التي كانوا ضحاياها .

الخاتمة

بعد إستعراضنا بالبحث و الدراسة لموضوع آليات البحث و التحقيق في الجرائم المعلوماتية ، إتضح لنا جليا مدى التحول الذي مس مجلات البحث في مجال العلوم الجنائية ، فقد تأثرت هذه الأخيرة بالتطور التكنولوجي و بالخصوص بتطبيقات تقنية المعلوماتية ، فقد حاولنا من خلال كل ما إستعرضناه إضفاء الطابع الفني و التقني بالقدر المستطاع إلى الطابع القانوني للبحث ، وذلك من خلال الإعتماد على مزيج من المصطلحات القانونية و العلمية المعلوماتية ، إضافة إلى عرض مزدوج من المفاهيم القانونية و المعلوماتية ، و كل ذلك بغرض إبراز مدى تقدم البحوث في المجال القانوني الجنائي و بالخصوص في مجال الإجراءات الجنائية المتعلقة بأعمال البحث و التحقيق ، و التي طالما تميزت بالطابع التقليدي المادي ،غير أن تأثر الجريمة بتطور نمط الحياة في ظل عصر تكنولوجيا المعلومات ،عجل بإستحداث مفاهيم و إجراءات قانونية حديثة تهدف إلى تطوير أعمال البحث و التحقيق في مجال الجرائم المعلوماتية ، بهدف ملاحقة جرائم و مجرمي المعلوماتية ضمانا لعدم فقدان السيطرة على إستعمالات تقنية المعلوماتية و عدم حيادها عن أهدافها الرئيسية المتمثلة في خدمة المصالح المعرفية للمجتمعات و الشعوب ، و يمكن لنا أن نوجز ما تضمنه بحثنا من نتائج منبثقة عن الإشكاليات المطروحة في مجال أعمال و وسائل البحث و التحقيق في الجرائم المعلوماتية فيما يلي:

- إن التقنية المعلوماتية أصبحت من أساسيات حياة الدول و الشعوب و لا يمكن تصور فكرة التخلي عنها ، نظرا لتزايد مجالات إستعمالاتها في كافة المجالات ، و ذلك بالرغم من كافة التهديدات التي تشكلها الجريمة المعلوماتية على أمن و سلامة نظمها و مستعمليها.
- يستحيل القضاء على الظاهرة الإجرامية المعلوماتية بشكل نهائي ، و ذلك لإتصالها المباشر بتقنية المعلوماتية ، ففكرة التخلي عن هذه التقنية هي الحل الوحيد لمشروع القضاء على الجريمة المعلوماتية ،

و ذلك بالرغم من درجة التطور التي آلت إليها المنظومة القانونية العقابية منها و الإجرائية في مجال مكافحة الجريمة المعلوماتية .

- ظهور فئة جديدة من المجرمين و الضحايا تحت و صفي " مجرمي المعلوماتية " و ضحايا الإجرام المعلوماتي " فالفئة الأولى أهم ما يميزها هو الذكاء و العلم و المعرفة ، و الخطورة الإجرامية في مجال المعلوماتية ، و ذلك بالرغم من خلو ملامحهم الشخصية من ملامح المجرمين المتعارف عليها في أصول علم الإجرام ، و هو ما يزيد من درجة خطورتهم و تهديدهم نظرا لكونهم خارج مجال الشك و الريبة مما يعزز ثقتهم في انفسهم على مواصلة نشاطهم الإجرامي و السعي إلى تطوير أساليبهم الإجرامية ، أما الفئة الثانية فعادة ما يميزها قلة المعرفة و التقدير بمجال المعلوماتية و هو ما يجعل منها أهدافا سهلة لمجرمي المعلوماتية .
- تنامي الظاهرة الإجرامية المعلوماتية و إزدياد حجم النشاط الإجرامي بشكل مفرط ، و تحولها من مجرد اعمال تهدف إلى قرصنة المعلومات إلى نشاط هادف ، هاجسه الأول تحقيق الربح المادي بإعتباره الباعث الرئيسي الذي يحرك مجرمي المعلوماتية و يغذي رغباتهم ، إضافة إلى أغراض أخرى تستجيب للواقع الحالي كالإرهاب الإلكتروني و النشاط الإجرامي المنظم ، فقد أصبحت الجماعات الإجرامية و الإرهابية تستغل شبكة الانترنت لأجل حصد موارد مالية و نشر أفكارها و إستغلال كل ذلك في ترهيب و ترويع الشعوب و الحكومات .
- تصنيف الجرائم المعلوماتية في صورة الإستغلال الجنسي للأطفال و كذلك جرائم الحض على الكراهية و التمييز العنصري ، من بين أخطر الجرائم نظرا لقلة حيلة و ضعف الضحايا في هذه الخالة ، لما قد تتسبب فيه من قيام نزعات بين الشعوب .

- على المستوى القانوني و التشريعي فإننا لاحظنا مدى الإهتمام الذي توليه الدول و الحكومات لهذا المجال من خلال التحديثات المستمرة و المتوالية للنصوص العقابية و الإجرائية ، بشكل متناسق مع تطور الأساليب الإجرامية المعلوماتية ، و هي الجهود التي لاحظنا غيابها عن أغلب التشريعات العربية إلا السعودي و الإماراتي منها ، و هو حال التشريع الجزائري الذي أصبح يميزه الجمود و القدم مقارنة بما آلت إليه الجريمة المعلوماتية من جهة، و التشريعات الغربية من جهة أخرى ، و كل ذلك بدعوى عدم تأثر المجتمع الجزائري بالظاهرة الإجرامية المعلوماتية بالشكل الذي يستوجب سن و تعديل النصوص على وجه الإستعجال ، و هي المعطيات و الحجج التي من شانها تشجيع مجرمي المعلوماتية على التصعيد من نشاطهم و تهديد المصالح العامة و الخاصة ، خصوصا و ان تقنية المعلوماتية أصبحت من التقنيات الأكثر شيوعا في الجزائر .
- إن إجراءات البحث و التحقيق المعلوماتي هي إجراءات من نوع خاص يشترط لمباشرتها التقييد بمجموعة من الشروط أهمها شرط التقييد بالنص الإجرائي الملائم ، لما قد تنطوي عليه هذه الإجراءات من مساس بالحريات الفردية و إطلاع على مستودع سر الأفراد، كالتصنت الإلكتروني و إعتراض البريد الإلكتروني ، و حجز للمعطيات و البيانات الشخصية ، و كل ذلك حفاظا على سلامة الإجراءات من طائلة البطلان و و كذلك حفاظا على حريات الأفراد و كرامتهم .
- تخضع إجراءات البحث و التحقيق المعلوماتي لإختصاص جهات متخصصة في التعامل مع الجرائم المعلوماتية ، تعتمد في تكوينها على مجموعة من المختصين في مجال المعلوماتية و كذلك في مجال التحقيق الجنائي ، مما يجعل منهم أفضل الأشخاص الذين يستطيعون التكفل بمهام البحث و التحقيق في الجرائم المعلوماتية ، نظرا لتقديرهم العلمي و المعرفي بالأساليب الإجرامية المعلوماتية ، و كذلك القواعد القانونية للتعامل بالشكل الشرعي مع الجريمة المعلوماتية ، إضافة إلى مراعاتهم لجملة

من القواعد العملية الإحتياطية منها و الأصلية عند مباشرة الإجراءات التي تهدف إلى جمع الأدلة، بشكل يكون الهدف منه ضمان حسن سير الإجراءات و الحفاظ على سلامتها من طائلة البطلان ، و كذا سلامة الأدلة من مخاطر التلف و الفقدان .

- تعتمد إجراءات البحث و التحقيق في مجال الجرائم المعلوماتية على القواعد الفنية العملية أكثر منه على القواعد الإجرائية القانونية ، فلا جدوى من النص دون توفر المهارة اللازمة في التعامل مع الجريمة المعلوماتية، كما ان حسن سير الإجراءات ذات الطبيعة الفنية و العملية يعتمد مباشرة على مدى توفر الوسائل المادية الضرورية من حواسيب متطورة و شبكات إتصال مؤمنة ، و برامج خاصة تسمح بتحصيل الدليل الإلكتروني ، تسهل من مهمة الخبير في مجال البحث و التحقيق المعلوماتي.
- يقترن نجاح إجراءات البحث و التحقيق في الجرائم المعلوماتية بمدى براعة و فعالية و جاهزية الجهات المختصة بمباشرة الإجراءات لتتبع الأدلة الإلكترونية ، و تحصيلها و حفظها بغرض عرضها على الجهات المختصة بتقديرها ، ذلك لأن الدليل الإلكتروني هو دليل جنائي من نوع خاص ، لا يشترك مع باقي الأدلة الجنائية في أي صفة مميزة ، فهو ذو طبيعة رقمية غير مادية ، كما انه قابل للفقدان من خلال تدميره أو محوه بكل سهولة و من اي مكان كان ، من قبل المجرم المعلوماتي ، او حتى من قبل المحققين ذاتهم خطأ منهم أو تقصيرا في التعامل بالقواعد الإحتياطية مع الأدلة الإلكترونية .
- تعاني إجراءات البحث و التحقيق من عدة عوائق تجعل من أمر مباشرتها او تنفيذها و إتمامها صعبا بل مستحيلا أحيانا و تتمثل هذه الصعوبات و العوائق فيما يلي :
- طبيعة الجريمة المعلوماتية في حد ذاتها ، فالطبيعة المعنوية للجريمة و إتخاذها من فضاء المعلوماتية ملجا لها ، يجعل من امر مكافحتها قانونيا أمرا بالغا في الصعوبة نظرا لتطورها الدائم و المستمر بشكل

يومي ، و هو ما لا يُتسنى تحقيقه من الناحية القانونية ، و هو ما يسمح لمجرمي المعلوماتية بخلق فضاء مناورة لأحكام القانون .

- ضعف المنظومة التشريعية في مواجهة الجريمة المعلوماتية ، من خلال عدم توفير المناخ القانوني الملائم ، سواء من ناحية النص التجريمي أو الإجرائي ، و هو ما يتسبب في خلق فجوات قانونية هائلة بين مجالي الجريمة المعلوماتية و التشريع ، و هو ما يعرقل خطة مكافحة الجريمة المعلوماتية ، بما فيها الإجراءات الخاصة بالبحث و التحقيق في هذا المجال ، نظرا لإفتقار الجهات المختصة بالبحث و التحقيق في مجال الجرائم المعلوماتية للسند القانوني المناسب.
- ضعف القدرات الأدائية للجهات المختصة بالبحث و التحقيق في الجرائم المعلوماتية ، إما لعدم تخصص أفرادها بمجال المعلوماتية و إعتمادهم على الطرق التقليدية لحل القضايا الإجرامية في التعامل مع الجريمة المعلوماتية ، مما يتسبب في فقدان الأدلة الإلكترونية و القضاء على معالم الجريمة ، أو العكس من ذلك أي تغليبهم للجانب الفني على القانوني مما يجعل من الإجراءات المتخذة و الأدلة المحصلة باطلة من الناحية القانونية ، أو قد يكون السبب ماديا بحتا من خلال عدم توفر الوسائل المادية الضرورية ممثلة في الحواسيب المتطورة و المزودة بأحدث البرامج في مجال ترصد و تتبع مجرمي الجرائم المعلوماتية .
- طبيعة الأدلة الإلكترونية و التي تتميز بقابلية الفقدان و سهولة المحو و التدمير من قبل المجرمين ، و ذلك بسسب قدرتهم الوصول إليها عبر الشبكات ، و من إي بقعة من الأرض و ذلك في حال عدم التعامل معها بالشكل المطلوب و السرعة اللازمة .
- إشكالية قلة التبليغات عن الجرائم المعلوماتية بسبب إتخاذ الضحايا لمواقف سلبية غالبا تجاه الجريمة المعلوماتية ، خشية منهم على سمعتهم أو لإنعدام معرفتهم بأن الأفعال التي كانوا ضحايا لها هي في

الأصل جرائم ، أو لإنعدام الثقة لديهم في الأجهزة الأمنية في قدرتها على إنصافهم ، و هي في مجملها عوائق تصعب م تزيد من تعقيد أعمال البحث و التحقيق في مجال الجرائم المعلوماتية ، و لذلك و بناء على كل ما إستعرضناه جاز لنا وضع و التنويه بمجموعة **من التوصيات** التي تساهم في حل الإشكاليات و العوائق التي صادفتنا في مجال البحث ، و التي نوجزها فيما يلي :

- وجوب إعتماد مصطلح " الجريمة المعلوماتية" بإعتباره المصطلح و التسمية الأكثر شيوعا ، و المتفق على مضمونها دوليا في وصف الظاهرة الإجرامية المعلوماتية ، و ذلك لما تحمله من وصف قانوني ذو طابع إجرامي له الأثر الوقائي على نفسية الجناة، و ذلك بدل المصطلح الذي إعتمده المشرع الجزائري تحت وصف " جرائم المساس بأنظمة المعالجة الآلية للمعطيات " التي تفتقد للدقة و تقود إلى التفكير في نوع آخر من الجرائم .
- العمل على التحسيس بخطورة الجريمة المعلوماتية على الأمن العام ، و أمن الأفراد من خلال إدراج مفهوم الجريمة المعلوماتية ضمن المقررات الدراسية و خصوصا منها الجامعية ، في مجال الحقوق و المعلوماتية ، و كذلك من خلال تنظيم ايام دراسية و تحسيسية لفائدة موظفي الشركات و المؤسسات خصوصا المالية منها ، من أجل وضعهم أمام واقع الجريمة المعلوماتية ، بإعتبارها خطرا يهدد أمن و سلامة النظم المعلوماتية لهذا النوع من المؤسسات بالدرجة الأولى ، بإعتبار أن الغرض الرئيسي لمجرمي المعلوماتية هو تحقيق الربح المادي، و ذلك من خلال تلقينهم صور و أنواع و أساليب الجرائم المعلوماتية، و سبل التصدي للهجمات الإلكترونية و كيفية التعامل معها.
- ضرورة العمل على تحسيس ضحايا الجرائم المعلوماتية بضرورة التبليغ عن أي جريمة معلوماتية قد يقعون ضحايا لها ، و ذلك من أجل السماح للجهات المكلفة بالبحث و التحقيق بالإطلاع على مدى جسامة و حقيقة الجريمة المعلوماتية ، إضافة إلى الإطلاع على كافة الأساليب الإجرامية الحديثة

المستعملة في مجال الجريمة المعلوماتية ، و التي يمكن ان تبقى محل خفاء في حال عدم تبليغ الضحايا عن الجرائم المعلوماتية التي تستهدفهم.

- **على المستوى التشريعي :**

- دعوة السلطات العليا إلى ضرورة الإنضمام إلى المعاهدة الدولية لمكافحة الجرائم المعلوماتية لسنة 2001(إتفاقية بودابست) ، و ذلك بإعتبارها إتفاقية مفتوحة للتوقيع و التصديق من قبل كافة الدول ، و ذلك حتى نستفيد من جملة الجهود التشريعية الدولية في مجال تعزيز أعمال البحث و التحقيق في الجرائم المعلوماتية.

- يجب و على وجه الإستعجال إستحداث نصوص قانونية متلائمة و مستوى التطور الذي آلت إليه تقنية المعلوماتية ، و درجة خطورة الجرائم المعلوماتية ، و ذلك اولا على مستوى قانون العقوبات الجزائري فالنصوص الواردة بموجب تعديل سنة 2009 ، نصوص قاصرة غير متكاملة و غير مضبوطة المصطلحات ، فنجد أن الأسلوب الغالب عليها هو أسلوب العمومية في التجريم و عدم الدقة في تفصيل النص التجريمي حسب كل جريمة بذاتها و أركانها ، كما نقف على غياب النص التجريمي المتعلق بعديد الجرائم المعلوماتية منها الإستغلال الجنسي للأطفال عبر شبكة الأنترنت ، إضافة إلى جرائم التحريض على الكراهية و العنف ضد الأقليات ، بالرغم من كون وسيلة الأنترنت و في الوقت الحالي هي من اهم الوسائل التي يستعين بها المجرمون من اجل تحقيق هذه الغايات الدنيئة ، إضافة إلى تشديد العقوبات في هذا المجال من أجل إحداث الأثر الوقائي و الردعي المرجو من إقرار قانون العقوبات.

- تعديل قانون الإجراءات الجزائية على وجه الإستعجال من خلال إدراج قسم خاص بأعمال البحث و التحقيق في الجرائم المعلوماتية ، و ذلك من خلال إفراد نصوص قانونية خاصة بالإجراءات الجزائية المتبعة خلال مرحلة البحث و التحري و كذلك التحقيق بشكل مفصل وواضح، يبين قواعد الإختصاص

النوعي و المحلي بدقة ووضوح ، إضافة إلى طبيعة الإجراءات المتخذة في هذا الشأن ، و ذلك للقضاء على كل لبس قد ينشأ جراء المزج بين النصوص العامة و الخاصة ، و ذلك تجسيدا للطبيعة الخاصة للجريمة المعلوماتية بفهومها الخاص ، ضمن فصول و احكام القانون الإجرائي .

- تعزيز عمل الجهات الأمنية و القضائية في مجال مكافحة الجرائم المعلوماتية ، و ذلك من خلال حسن تدريب الكفاءات العاملة على طبيعة الإجراءات المتخذة في مجال الجرائم المعلوماتية ومدى خصوصية هذا النوع من الجرائم و المجرمين في آن واحد ، إضافة إلى تعزيزهم بأحدث الوسائل التكنولوجية في مجال المعلوماتية من حواسيب و برامج معلوماتية ، تسمح لهم بتأدية مهامهم على اكمل وجه.
- وضع سجل أمني إلكتروني يتضمن قائمة بمجرمي المعلوماتية يسمح بوضعهم تحت المراقبة الأمنية ، أي رصد نشاطاتهم المعلوماتية المشبوهة عبر الشبكة، و التي تنذر بوقوع جريمة معلوماتية .

إذن كانت هذه جملة من المقترحات التي يرى الباحث بضرورة تبنيها و تجسيدها على ارض الواقع من اجل الوصول إلى ضمان فعالية قصوى في عمل الجهات المختصة بالبحث و التحقيق في الجرائم المعلوماتية ، و بالتالي تجسيد السياسة الهادفة غلى تامين فضاء المعلوماتية ، و مكافحة الجرائم المعلوماتية .

ملاحق البحث

ملحق البحث رقم 01

قاموس المصطلحات المعلوماتية

المصطلح باللغة العربية	المصطلح باللغة الأجنبية	شرح مضمون المصطلح
تقنية ADSL	ADSL	تقنية ربط بالشبكات (شبكة الأنترنت) ، عن طريق استعمال الهاتف الثابث ، تمنح قوة تدفق أقرب لتلك التي توفرها تقنية الالياف البصرية.
عنوان بريد إلكتروني	Adresse Electronique	هو عبارة عن عنوان إلكتروني مشابه للعنوان البريدي ، يُتداول عبره البريد الإلكتروني ، يتكون من إسم المستخدم و عنوان على شبكة الأنترنت مفصولين بعلامة مميزة هي @.
تطبيق معلوماتي	Application	برنامج موضوع خصيصا من أجل مساعدة المستخدم على تنفيذ بعض المهام الخاصة على الحاسوب كمعالجة النصوص مثلا.
ثنائي	Binaire	نظام رقمي يعتمده الحاسوب يستخدم فيه لغة رقمي الصفر و الواحد كأساس للعد .
بت	Bit	رقم ثنائي يشير إلى أصغر وحدة من المعلومات التي يتم نقلها عبر الحاسوب ، في شكل نبضة مضيئة On أو مطفأة Off يرمز لها بالواحد أو الصفر .
بت في الثانية	Bits par seconde (BPS)	وحدة قياس سرعة وسيط النقل ، أي عدد البتات التي تمر عبر الوسيط في الثانية الواحدة .
بايت	Byte	كلمة ثنائية للدلالة علة وحدة قياس ثنائية ، تتكون من 08 بتات Bits.

عميل	Client	برنامج أو حاسوب يتصل بالخادم و يطلب منه معلومات .
عميل خادم	Client /serveur	طريقة توزيع المعلومات و الملفات ، تعتمد على قيام برنامج يعرف بالخادم المركزي بتخزين الملفات و المعلومات و إتاحتها لمتطلبات برنامج العميل
كعكة كوكي	Cookie	عبارة عن ملفات و سجل بيانات تسجل على القرص الصلب للحاسوب عند إتصاله بحواسيب أخرى ، تتيح هذه البيانات للمزود Serveur بمعرفة المواقع التي زارها المستخدم في الأونة الأخيرة .
بيانات	Data	هي كل انواع المعلومات أيا كان نوعها و التي يتم تخزينها و نقلها أو معالجتها بواسطة الحاسوب .
قاعدة بيانات	Data base	جملة من البيانات المحفوظة على ذاكرة الحاسوب التي يمكن الوصول إليها عن طريق عملية البحث .
فك التشفير	Décrypte	إعادة البيانات إلى ما كانت عليه قبل تشفيرها Encrypt، بحيث يسمح ذلك بإستعراضها و قرائتها

رقمي	Digital Numérique	كل تمثيل للقيم المسموعة أو المرئية إلى بتات Bits، فالقرص المظغوط CD هو وسيط تخزين رقمي لأن الأصوات التي يتم تحويلها إلى بتات Bits ثم يتم تخزينها عليه ، و عند تشغيله يقوم المشغل Player بإعادة تحويل تلك البتات Bits إلى إشارات تناظرية Analog ثم يرسلها عبر السماعات في شكل أصوات.
تحميل	Download Téléchargement	عملية نقل ملف عبر شبكة الأنترنت من حاسوب آخر بعيد إلى حاسوب المستخدم ، قد يكون الملف مقروءا أو مسموعا أو مرئيا أو تطبيقا أو برنامجا معلوماتيا.
تشفير	Encryption Cryptage	تعديل محتويات ملف أو رسالة بإستخدام كلمة سر أو مرور ، بحيث لا يستطيع أي شخص قراءتها إلا من كان لديه شفرة أو مفتاح المرور.
بريد إلكتروني	Electronique Mail	يختصر المصطلح عادة إلى Email و يقصد به الرسائل المتبادلة إلكترونيا من حاسوب لأخر عبر شبكة الأنترنت.
بروتوكول نقل الملفات	File Transfer Protocol (FTP)	أحد أكثر بروتوكولات نقل الملفات شيوعا ، يستخدم لنقل الملفات من حاسوب لأخر عبر الأنترنت ، عبر مزودات FTP التي تسمح للمستخدمين بجلب الملفات و تبادلها.

جدار النار أو حاجز النار	Fire Wall Par Feu	أحد الإحتياطات الأمنية على شبكة الأنترنت ، يحمي المعلومات أو يمنع الوصول إليها ، كما يضمن عدم إلحاق الضرر بالمستخدمين من خلال حماية نظم التشغيل الخاصة بهم ، يعمل الجدار الناري في شكل نظام أمني ينظم حركة مرور المعلومات عند حدوث إتصال بين شبكتين على الأقل ، فيسمح لحزم البيانات بالمرور أو يمنعها بين الشبكتين ، و ذلك إعتمادا على مجموعة من القواعد التي يحددها مدير الشبكة مثل إسم المستخدم و كلمة السر .
لغة ترميز النص التشعبي	Hyper Text Markup Language (HTML)	لغة تستخدم في إنشاء صفحات الويب ، تتكون من نص عادي ، و علامات تعرف بـ Tags تخبر المستخدم عن كيفية عرض النص على شاشة الحاسوب .
إرتباط تشعبي	Hyperlink	علامات مميزة على صفحات الويب تسمح بالإنتقال من صفحة إلى أخرى ، و من موقع لأخر على شبكة الويب
نص تشعبي	HyperText	نص يحتوي على مجموعة من الوصلات الإرتباطية تسمح للمستخدم من أن يتخطى النص المعروض أمامه و يقرأ أي نص أخر حسب أي ترتيب يرغب فيه

أنترنت	Internet	شبكة دولية بها ألاف الشبكات الفرعية المرتبطة بها بإستخدام برتوكول TCP/IP ، تربط هذه الشبكة بين أجهزة الحواسيب من أجل تبادل المعلومات المتوفرة على هذه الشبكة
برتوكول الأنترنت	Internet Protocol (IP)	هو بروتوكول يتحكم في كيفية إنتقال البيانات من مضيف إلى آخر عبر الأنترنت ، من خلال العمل مع برتوكول التحكم في نقل البيانات Transmission Control Protocol (TCP)، لكي يتم ضمان نقل البيانات بصورة صحيحة على الأنترنت ، برتوكول الأنترنت هو المسؤول عن تراسل حزم البيانات و ضمان توجيهها إلى أهدافها ، من خلال دمغها بعنوان مما يتيح توجيهها إلى وجهتها .
عنوان بروتوكول الأنترنت	Adresse internet Protocol (Adresse IP)	يعرف أيضا بالعنوان الرباعي المنقط ، و هو عنوان رقمي خاص بكل حاسوب يضمن التعريف به على شبكة الانترنت و تحديد موقعه ، يتكون من أربعة مجموعات من الأرقام تفصل بينها النقاط
ميجابت	Mb	إختصار لكلمة Megabit و هي مليون بت Bit
ميجابت في الثانية	Mbps	وحدى لقياس عرض الحزمة و تعني كلمة ميجا : الرقم 10 أس 6 .

مودم	Modem	إختصار لكلمة Modulateur و هو جهاز يربط الحاسوب بشبكة الأنترنت و منه ببقية الحواسيب المتصلة بالشبكة ، يعمل من خلال نقل البيانات بعد تحويلها من رقمية إلى تناظرية قابلة للنقل عبر خط الهاتف في حال إرسالها و العكس من ذلك في حال إستقبالها.
بروتوكول	Protocol	مجموعة من القواعد المتفق عليها و التي تتيح إتصال البرامج و الأجهزة المختلفة و غير المتوافقة مع بعضها البعض ، فهي اللغة التي تتخاطب بها الحواسيب المتصلة عبر الشبكة بهدف تبادل المعلومات ، فهو و بلغة تقنية الوصف الرسمي للقواعد التي ينبغي على حاسوبين إتباعها لتبادل المعلومات و الرسائل .
خادم البروكسي	Proxy Serveur	إحتياط أمني يتيح للمستخدم الموجود خلف الجدار الناري من إستعراض محتويات الويب دون تعريض محتويات الشبكة الخاصة لخطر الإطلاع عليها .
الخادم	Serveur	برنامج أو جهاز حاسوب يوفران المعلومات بالنسبة للحواسيب أو البرامج العميلة المتصلة به .
مزود الخدمة	Service Provider	الشركة التي توفر الوصول المباشر للأنترنت

بروتوكول التحكم بنقل البيانات / بروتوكول أنترنت	Transmission Control Protocol/ Internet Protocol (TCP/IP)	مجموعة من البروتوكولات التي تحدد نظام نقل البيانات عبر شبكة الأنترنت ، توصف بأنها الغراء الذي يشد أجزاء الأنترنت بعضها لبعض ، فتحقق الترابط بين شبكات متباعدة فيزيائيا بصورة مباشرة لتشكل معا شبكة إفتراضية وحدة تغرف بإسم " الأنترنت"
بروتوكول التحكم بنقل البيانات	Transmission Control Protocol (TCP)	أحد بروتوكولات مجموعة TCP/IP يوفر وسيلة نقل موثوقة للبيانات غبر شبكة الأنترنت ، فبفضله يمكن لحاسوب متصل بالشبكة الأنترنت أن يقيم تواصلا مع حاسوب آخر و يتبادل معه المعلومات .
عنوان الموارد الموحد	Uniform Resource Locator (URL)	مؤشر يدل على مكان وجود صفحة أو أي نوع أخر من الموارد ضمن فضاء الويب (WEB).
مستخدم	User	أي شخص يقوم بالدخول إلى نظام تشغيل الحاسوب أو إحدى الشبكات
إسم المستخدم	Username	هو وسيلة الدخول أي الإسم الذي يلج به المستخدم إلى النظام المعلوماتي ، مثاله الجزء الأول من العنوان الإلكتروني الذي يسبق علامة @.

فيروس	Virus	برنامج يقوم بإحداث تلف متعمد على الحاسوب و عادة ما يكون في صورة برنامج خفي على الشبكة أو لصيق بأحد البرامج .
الويب	Worled Wide Web(WEB)	عبارة عن مجموعة من المستندات(وثائق ، صور ، فيديوهات.....) المتصلة في شكل نصوص تشعبية HTML ، متواجدة على أجهزة خادم الويب ، يمكن الوصول إليها عن طريق عناوين الأنترنت URL و قد تم إستحداث الويب كمصدر للمستندات المباشرة بواسطة علماء الفيزياء في CERN أو المعمل الأوربي للفيزياء الجزيئية بسويسرا .
مستعرض الويب	Web Browser	برنامج عميل خاص بالويب يعمل على عرض مستندات الويب بلغة HTML و المستندات الأخرى ، يتيح للمستخدم الإطلاع على مختلف المستندات من خلال تتبع إرتباطات النص التشعبي و اشهره Internet Explorer / Mozila Fire Fox
صفحة ويب	Page Web	أحد مستندات HTML يحتوي على إرتباطات تشعبية إلى مستندات أخرى على الويب ، و تقول فكرة التجول و الإبحار على شبكة الويب على فطرة تتبع الإرتباطات من صفحة لأخرى
موقع ويب	Web Site	أحد المواقع على شبكة الأنترنت و الذي يستضيف خادم ويب .

ملحق البحث رقم 02

القانون 09/04 المتعلق بالوقاية من الجرائم المعلوماتية

قوانين

قانون رقم 09 – 04 مؤرّخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

إن رئيس الجمهورية،

– بناء على الدستور، لا سيما المواد 119 و120 و122 – 7 و126 منه،

– وبمقتضى الأمر رقم 66 – 155 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 66 – 156 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 75 – 58 المؤرّخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون المدني، المعدّل والمتمّم،

– وبمقتضى القانون رقم 2000 – 03 المؤرّخ في 5 جمادى الأولى عام 1421 الموافق 5 غشت سنة 2000 الذي يحدّد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 03 – 05 المؤرّخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003 والمتعلق بحقوق المؤلف والحقوق المجاورة،

– وبمقتضى القانون رقم 08 – 09 المؤرّخ في 18 صفر عام 1429 الموافق 25 فبراير سنة 2008 والمتضمن قانون الإجراءات المدنية والإدارية،

– وبعد رأي مجلس الدولة،

– وبعد مصادقة البرلمان،

يصدر القانون الآتي نصه :

الفصل الأول
أحكام عامة
الهدف

المادّة الأولى : يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المصطلحات

المادّة 2 : يقصد في مفهوم هذا القانون بما يأتي :

أ – الجرائم المتصلة بتكنولوجيات الإعلام والاتصال : جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية،

ب – منظومة معلوماتية : أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين،

ج – معطيات معلوماتية : أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها،

د – مقدمو الخدمات :

1 – أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات،

2 – وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها،

هـ – المعطيات المتعلقة بحركة السير: أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة،

و – الاتصالات الإلكترونية : أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.

مجال التطبيق

المادّة 3 : مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

الفصل الثاني

مراقبة الاتصالات الإلكترونية

الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية

المادّة 4 : يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية :

أ - للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة،

ب - في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني،

ج - لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية،

د - في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة.

عندما يتعلق الأمر بالحالة المنصوص عليها في الفقرة "أ" من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه، إذنا لمدة ستة (6) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة "أ" من هذه المادة موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتهما، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

الفصل الثالث

القواعد الإجرائية

تفتيش المنظومات المعلوماتية

المادّة 5 : يجوز للسلطات القضائية المختصة وكذا ضبّاط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه، الدخول، بغرض التفتيش، ولو عن بعد، إلى :

أ - منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب - منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة "أ" من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها، انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

حجز المعطيات المعلوماتية

المادّة 6 : عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة

تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.

غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

الحجز عن طريق منع الوصول إلى المعطيات

المادّة 7 : إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 6 أعلاه، لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

المعطيات المحجوزة ذات المحتوى المجرم

المادّة 8 : يمكن السلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة ، لا سيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك.

حدود استعمال المعطيات المتحصل عليها

المادّة 9 : تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.

الفصل الرابع

التزامات مقدمي الخدمات

مساعدة السلطات

المادّة 10 : في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه، تحت تصرف السلطات المذكورة.

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.

حفظ المعطيات المتعلقة بحركة السير

المادّة 11 : مع مراعاة طبيعة ونوعية الخدمات، يلتزم مقدمو الخدمات بحفظ :

أ - المعطيات التي تسمح بالتعرف على مستعملي الخدمة،

ب - المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،

ج - الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال،

د - المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها،

هـ - المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ" من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه.

تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل.

دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (6) أشهر إلى خمس (5) سنوات وبغرامة من 50.000 دج إلى 500.000 دج.

يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات.

تحدد كيفيات تطبيق الفقرات 1 و2 و3 من هذه المادة، عند الحاجة، عن طريق التنظيم.

الالتزامات الخاصة بمقدمي خدمة "الإنترنت"

المادّة 12 : زيادة على الالتزامات المنصوص عليها في المادة 11 أعلاه، يتعين على مقدمي خدمات "الإنترنت" ما يأتي :

أ – التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن،

ب – وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.

الفصل الخامس

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته

إنشاء الهيئة

المادّة 13 : تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم.

مهام الهيئة

المادّة 14 : تتولى الهيئة المذكورة في المادة 13 أعلاه، خصوصا المهام الآتية :

أ – تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته،

ب – مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية،

ج – تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

الفصل السادس

التعاون والمساعدة القضائية الدولية

الاختصاص القضائي

المادّة 15 : زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني.

المساعدة القضائية الدولية المتبادلة

المادّة 16 : في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني.

يمكن، في حالة الاستعجال، ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أوالبريد الإلكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها.

تبادل المعلومات واتخاذ الإجراءات التحفظية

المادّة 17 : تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقات الدولية الثنائية ومبدأ المعاملة بالمثل.

القيود الواردة على طلبات المساعدة القضائية الدولية

المادّة 18 : يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام.

يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب.

المادّة 19 : ينشر هذا القانون في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009.

عبد العزيز بوتفليقة

ملحق البحث رقم : 03

المرسوم الرئاسي رقم 15-261 المحدد لتشكيلة و تنظيم و كيفيات عمل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها

مراسيم تنظيميّة

مرسوم رئاسي رقم 15-261 مؤرّخ في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر سنة 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

إنّ رئيس الجمهورية،

– بناء على الدستور، لا سيما المواد 39 و77 (1 و2 و8) و125 (الفقرة الأولى) منه،

– وبمقتضى القانون العضوي رقم 04-11 المؤرخ في 21 رجب عام 1425 الموافق 6 سبتمبر سنة 2004 والمتضمن القانون الأساسي للقضاء،

– وبمقتضى الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية ، المعدل والمتمم،

– وبمقتضى الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدل والمتمم،

– وبمقتضى القانون رقم 90-21 المؤرخ في 24 محرم عام 1411 الموافق 15 غشت سنة 1990 والمتعلق بالمحاسبة العمومية، المعدل والمتمم،

– وبمقتضى القانون رقم 2000-03 المؤرخ في 5 جمادى الأولى عام 1421 الموافق 5 غشت سنة 2000 الذي يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، المعدل والمتمم،

– وبمقتضى القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

يرسم ما يأتي :

الفصل الأول

أحكام عامة – تعاريف

المادّة الأولى : تطبيقا لأحكام المادة 13 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمذكور أعلاه، يهدف هذا المرسوم إلى تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي تدعى في صلب النص "الهيئة".

المادّة 2 : الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، توضع لدى الوزير المكلف بالعدل.

المادّة 3 : يحدد مقر الهيئة بمدينة الجزائر.

المادّة 4 : تمارس الهيئة المهام المنصوص عليها في المادة 14 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، تحت رقابة السلطة القضائية، طبقا لأحكام التشريع الساري المفعول، لا سيما منها قانون الإجراءات الجزائية والقانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمذكور أعلاه.

تكلف الهيئة، في ظل احترام الأحكام التشريعية المبينة أعلاه على الخصوص، بما يأتي :

– اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

– تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

– مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية،

– ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة، تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى،

– تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية،

– السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها،

– تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال،

– المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال،

– المساهمة في تحديث المعايير القانونية في مجال اختصاصها.

المادّة 5 : يقصد في مفهوم هذا المرسوم بما يأتي :

– "**الاتصالات الإلكترونية**" : كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها عن طريق أي وسيلة إلكترونية، بما في ذلك وسائل الهاتف الثابت والنقال،

– "**مستخدمو الهيئة**" : المستخدمون الذين يمارسون عملهم بالتوقيت الكامل في الهيئة مهما كان وضعهم القانوني الأصلي.

الفصل الثاني

تشكيلة الهيئة وتنظيمها

المادّة 6 : تضم الهيئة :

– لجنة مديرة،

– مديرية عامة،

– مديرية للمراقبة الوقائية واليقظة الإلكترونية،

– مديرية للتنسيق التقني،

– مركز للعمليات التقنية،

– ملحقات جهوية.

المادّة 7 : يرأس اللجنة المديرة الوزير المكلف بالعدل، وتتشكل من الأعضاء الآتي ذكرهم :

– الوزير المكلف بالداخلية،

– الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال،

– قائد الدرك الوطني،

– المدير العام للأمن الوطني،

– ممثل عن رئاسة الجمهورية،

– ممثل عن وزارة الدفاع الوطني،

– قاضيان من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

يعين ممثلا رئاسة الجمهورية ووزارة الدفاع الوطني بموجب مرسوم رئاسي.

المادّة 8 : تكلف اللجنة المديرة على الخصوص، بما يأتي :

– توجيه عمل الهيئة والإشراف عليه ومراقبته،

– دراسة كل مسألة تخضع لمجال اختصاص الهيئة، لا سيما فيما يتعلق بتوفر شروط اللجوء للمراقبة الوقائية للاتصالات الإلكترونية المنصوص عليها في المادة 4 من القانون رقم 09–04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمذكور أعلاه،

– ضبط برنامج عمل الهيئة وتحديد شروط وكيفيات تنفيذه،

– القيام دوريا بتقييم حالة الخطر في مجال الإرهاب والتخريب والمساس بأمن الدولة، للتمكن من تحديد مشتملات عمليات المراقبة الواجب القيام بها والأهداف المنشودة بدقة ،

– اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

– دراسة مشروع النظام الداخلي للهيئة والموافقة عليه،

– دراسة مشروع ميزانية الهيئة والموافقة عليه،

– دراسة التقرير السنوي لنشاطات الهيئة والمصادقة عليه،

– إبداء رأيها في كل مسألة تتصل بمهام الهيئة،

– تقديم كل اقتراح مفيد يتصل بمجال اختصاص الهيئة.

المادّة 9 : يدير المديرية العامة مدير عام يعين بموجب مرسوم رئاسي. وتنهى مهامه حسب الأشكال نفسها.

المادّة 10 : يتولى المدير العام الصلاحيات الآتية على الخصوص :

– السهر على حسن سير الهيئة،

– السهر على تنفيذ برنامج عمل الهيئة،

– تنشيط نشاطات هياكل الهيئة وتنسيقها ومتابعتها ومراقبتها،

– تحضير اجتماعات اللجنة المديرة،

– تمثيل الهيئة لدى السلطات والمؤسسات الوطنية والدولية،

– تمثيل الهيئة لدى القضاء وفي جميع أعمال الحياة المدنية،

– ممارسة السلطة السلّمية على مستخدمي الهيئة.

– السهر على احترام قواعد حماية السر في الهيئة،

– السهر على القيام بإجراءات التأهيل وأداء اليمين فيما يخص المستخدمين المعنيين في الهيئة،

– إعداد التقرير السنوي لنشاطات الهيئة وعرضه على اللجنة المديرة للمصادقة عليه،

– ضمان التسيير الإداري والمالي للهيئة.

المادّة 11 : تكلف مديرية المراقبة الوقائية واليقظة الإلكترونية على الخصوص، بما يأتي :

– تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية، من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بناء على رخصة مكتوبة من السلطة القضائية وتحت مراقبتها طبقا للتشريع الساري المفعول،

– إرسال المعلومات المحصل عليها من خلال المراقبة الوقائية إلى السلطات القضائية ومصالح الشرطة القضائية المختصة،

– تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة وجمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم،

– جمع ومركزة واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

– تنظيم و/أو المشاركة في عمليات التوعية حول استعمال تكنولوجيات الإعلام والاتصال، وحول المخاطر المتصلة بها،

– تنفيذ توجيهات اللجنة المديرة،

– تزويد السلطات القضائية ومصالح الشرطة القضائية، تلقائيا أو بناء على طلبها، بالمعلومات والمعطيات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال،

– وضع مركز العمليات التقنية والملحقات الجهوية قيد الخدمة والسهر على حسن سيرها وكذا الحفاظ على الحالة الجيدة لمنشآتها وتجهيزاتها ووسائلها التقنية،

– تطبيق قواعد الحفاظ على السر في نشاطاتها.

المادّة 12 : تكلف مديرية التنسيق التقني على الخصوص، بما يأتي :

– إنجاز الخبرات القضائية في مجال اختصاص الهيئة،

– تكوين قاعدة معطيات تحليلية للإجرام المتصل بتكنولوجيات الإعلام والاتصال واستغلالها،

– إعداد الإحصائيات الوطنية المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال،

– القيام بمبادرة منها أو بناء على طلب اللجنة المديرة، بكل دراسة أو تحليل أو تقييم يتعلق بصلاحياتها،

– تسيير منظومة الإعلام للهيئة وإدارتها.

المادّة 13 : يزود مركز العمليات التقنية بالمنشآت والتجهيزات والوسائل المادية وكذا بالمستخدمين التقنيين الضروريين لتنفيذ العمليات التقنية لمراقبة الاتصالات الإلكترونية.

ويتبع هذا المركز مديرية المراقبة الوقائية واليقظة الإلكترونية ويتم تشغيله من طرفها.

المادّة 14 : يتم تشغيل الملحقات الجهوية من طرف مديرية المراقبة الوقائية واليقظة الإلكترونية التي تتبعها.

المادّة 15 : يحدد التنظيم الداخلي لهياكل الهيئة بموجب قرار مشترك بين الوزراء المكلفين بالعدل، والدفاع الوطني، والداخلية.

الفصل الثالث

كيفيات سير الهيئة

المادّة 16 : تجتمع الهيئة المديرة بناء على استدعاء من رئيسها أو بناء على طلب أحد أعضائها.

المادّة 17 : تعد الهيئة نظامها الداخلي وتصادق عليه.

المادّة 18 : تزود الهيئة بقضاة وفقا للشروط والكيفيات المنصوص عليها بموجب التشريع الساري المفعول.

كما تزود بضباط وأعوان للشرطة القضائية من المصالح العسكرية للاستعلام والأمن والدرك الوطني والأمن الوطني، يحدد عددهم بموجب قرارات مشتركة بين الوزراء المكلفين بالعدل، والدفاع الوطني، والداخلية.

وتزود أيضا بمستخدمي الدعم التقني والإداري، ويجلب هؤلاء المستخدمون من ضمن مستخدمي المصالح العسكرية للاستعلام والأمن والدرك الوطني والأمن الوطني.

المادّة 19 : يمكن أن تستعين الهيئة بأي خبير أو أي شخص يمكن أن يعينها في أعمالها .

المادّة 20 : تؤهل الهيئة لكي تطلب من أي جهاز أو مؤسسة أو مصلحة كل وثيقة أو معلومة ضرورية لإنجاز المهام المسندة إليها.

المادّة 21 : قصد الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة، تكلف الهيئة حصريا بمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية تحت سلطة قاض مختص، ووفقا للأحكام المنصوص عليها في المادة 4 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمذكور أعلاه.

المادّة 22 : يمكن الهيئة لتنفيذ عملية لمراقبة الاتصالات الإلكترونية، أن تضع وحدة مراقبة واحدة أو أكثر، تزود بالوسائل والتجهيزات التقنية الضرورية.

تتكون الوحدة من مستخدمين تقنيين يعملون تحت إدارة ومراقبة قاض يساعده ضابط واحد من الشرطة القضائية أو أكثر ينتمي للهيئة.

تمتثل الوحدة في عملها إلى أحكام التشريع الساري المفعول وشروط الرخصة المسلّمة من الشرطة القضائية.

وتحرر أشغالها في محضر يعد طبقا لأحكام قانون الإجراءات الجزائية.

المادّة 23 : لا يمكن أن يشارك في عملية لمراقبة الاتصالات الإلكترونية إلا أعضاء الوحدة أو الوحدات التي أوكلت لها السلطة القضائية هذه المهمة.

يتخذ مسؤول الوحدة أثناء سير العملية كل التدابير اللازمة، بالاتصال مع المسؤولين المعنيين في الهيئة، من أجل ضمان سرية العملية وحماية المعلومات المستقاة من المراقبة.

المادّة 24 : تحفظ المعلومات المستقاة أثناء عمليات المراقبة، خلال حيازتها من الهيئة، وفقا للقواعد المطبقة على حماية المعلومات المصنفة.

المادّة 25 : تسجل الاتصالات الإلكترونية التي تكون موضوع مراقبة، وتحرر وفقا للشروط والأشكال المنصوص عليها في قانون الإجراءات الجزائية.

تسلّم التسجيلات والمحررات إلى السلطات القضائية وإلى مصالح الشرطة القضائية المختصة وتحتفظ السلطات القضائية، دون سواها بهذه المعطيات أثناء المدة القانونية المنصوص عليها في التشريع الساري المفعول.

المادّة 26 : يجب، تحت طائلة العقوبات الجزائية المنصوص عليها في التشريع الساري المفعول، ألا تستخدم المعلومات والمعطيات التي تستلمها أو تجمعها الهيئة، لأغراض أخرى غير تلك المتعلقة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وذلك وفقا للأحكام المنصوص عليها في القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمذكور أعلاه.

المادّة 27 : يلزم مستخدمو الهيئة بالسرّ المهني وواجب التحفظ .

ويخضع المستخدمون من بينهم الذين يدعون إلى الاطلاع على معلومات سرّية إلى إجراءات التأهيل.

المادّة 28 : يؤدي مستخدمو الهيئة الذين يدعون إلى الاطلاع على المعلومات السرّية، اليمين أمام المجلس القضائي، قبل تنصيبهم، الآتي نصه :

"أقسم بالله العليّ العظيم أن أقوم بعملي أحسن قيام، وأن أخلص في تأدية مهنتي، وأن أكتم الأسرار والمعلومات أيا كانت التي أطلع عليها أثناء قيامي بعملي أو بمناسبته، وأن أسلك في كل الظروف سلوكا شريفا".

المادّة 29 : يوضع مستخدمو الهيئة تحت سلطة المدير العام.

المادّة 30 : يمكن أن يقوم القضاة وضباط الشرطة القضائية التابعون للهيئة أثناء ممارستهم لوظائفهم أو بمناسبتها، طبقا للشروط والكيفيات المنصوص عليها في التشريع الساري المفعول، ولا سيما قانون الإجراءات الجزائية، بتفتيش أي مكان أو هيكل أو جهاز بلغ إلى علمهم أنه يحوز و/أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الإلكترونية.

وفي حالة معاينة أفعال يمكن وصفها جزائيا، تخطر الهيئة النائب العام المختص للقيام بالمتابعات المحتملة.

المادّة 31 : يمكن أن تطلب الهيئة مساعدة موظفين مختصين من الوزارات المعنية في مجال تكنولوجيات الإعلام والاتصال، طبقا للشروط والكيفيات المحددة في التنظيم الساري المفعول.

المادّة 32 : يرفع رئيس اللجنة المديرة للهيئة إلى رئيس الجمهورية تقارير فصلية عن نشاطات الهيئة.

الفصل الرابع

أحكام مالية

المادّة 33 : يعد المدير العام ميزانية الهيئة ويعرضها على اللجنة المديرة للموافقة عليها.

تسجل ميزانية الهيئة في الميزانية العامة للدولة طبقا للتشريع والتنظيم الساريي المفعول.

ويكون المدير العام هو الآمر بصرف ميزانية الهيئة.

المادّة 34 : تشتمل ميزانية الهيئة على باب للإيرادات وباب للنفقات.

في باب الإيرادات :

- إعانات الدولة.

في باب النفقات :

- نفقات التسيير،
- نفقات التجهيز.

المادّة 35 : تمسك محاسبة الهيئة وفق قواعد المحاسبة العمومية.

يتولى مسك المحاسبة عون محاسبة يعينه أو يعتمده الوزير المكلف بالمالية.

المادّة 36 : يمارس المراقبة المالية للهيئة مراقب مالي يعينه الوزير المكلف بالمالية.

الفصل الخامس

أحكام قانونية أساسية

المادّة 37 : يعيّن مدير المراقبة الوقائية واليقظة الإلكترونية ومدير التنسيق التقني بموجب مرسوم رئاسي. وتنهى مهامهما حسب الأشكال نفسها.

المادّة 38 : يبقى ضباط وأعوان الشرطة القضائية وكذا المستخدمون التابعون للوزارات المعنية والممارسون وظائفهم في الهيئة خاضعين للأحكام التشريعية والتنظيمية والقانونية الأساسية المطبقة عليهم.

المادّة 39 : يستفيد مستخدمو الهيئة، طبقا للتشريع الساري المفعول، من حماية الدولة من التهديدات أو الضغوط أو الإهانات، مهما تكن طبيعتها، التي قد يتعرضون لها بسبب أو بمناسبة قيامهم بمهامهم.

المادّة 40 : تحدد طريقة صرف الرواتب والنظام التعويضي المطبقين على مستخدمي الهيئة بموجب نص خاص يحدد تصنيف الوظائف في الهيئة.

الفصل السادس

أحكام خاصة ونهائية

المادّة 41 : تمارس الهيئة الحصرية في مجال مراقبة الاتصالات الإلكترونية تحت مراقبة قاض مختص، باستثناء الحالات المنصوص عليها في قانون الإجراءات الجزائية.

وزيادة على ذلك، وما عدا الحالات المبيّنة في الفقرة السابقة، لا يمكن أن تستورد أو تقتني أو تحوز أو تستعمل الوسائل والتجهيزات التقنية لمراقبة الاتصالات الإلكترونية إلا الهيئة، أو عند الاقتضاء، سلطة ضبط الاتصالات السلكية واللاسلكية وكذا المؤسسة العمومية المكلفة بشبكات الاتصالات، وذلك باستثناء أي هيئة أو مؤسسة أو شخص.

يتولى الأعوان المؤهلون في الهيئة ووحداتها المكلفة بالمراقبة، لصالح ضباط الشرطة القضائية، الجوانب التقنية للعمليات المنصوص عليها في قانون الإجراءات الجزائية.

المادّة 42 : تحول إلى الهيئة نشاطات مراقبة الاتصالات الإلكترونية التي كانت تمارسها في السابق هيئات وطنية أخرى.

تحدد كيفيات تطبيق هذه المادة بموجب نص خاص.

المادّة 43 : ينشر هذا المرسوم في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر سنة 2015.

عبد العزيز بوتفليقة

قائمة المراجع

قائمة المصادر و المراجع.

❖ أولا: المصادر القانونية.

I. الإتفاقيات و المعاهدات الدولية .

1) إتفاقية بودابست لمكافحة الجرائم المعلوماتية – المنبثقة عن اجتماع المجلس الأوربي ببودابست – المجر تحت رقم 185– بتاريخ 21 نوفمبر 2001.

2) البروتوكول الإضافي لاتفاقية بودابست المتعلق بتجريم السلوكات الماسة بالكرامة الإنسانية و المحرضة على أعمال العنف و الكراهية و العنصرية بواسطة الأنظمة المعلوماتية– المنبثقة عن اجتماع المجلس الأوربي بستراسبورغ– فرنسا تحت رقم 189 بتاريخ 2003/01/28 .

3) الاتفاقية العربية لمكافحة جرائم تقنية المعلومات– المنبثقة عن اجتماع مجلس الوزراء الداخلية و العدل العرب بصفة مشتركة– بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة – مصر بتاريخ 2010/12/21.

II. الدساتير و القوانين :

1) دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 1996 المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية رقم 76 المؤرخة في 8 ديسمبر 1996 و المعدل بـ:

- القانون رقم 02–03 المؤرخ في 10 أفريل 2002 الجريدة الرسمية رقم 25 المؤرخة في 14 أفريل 2002.
- القانون رقم 08–19 المؤرخ في 15 نوفمبر 2008 الجريدة الرسمية رقم 63 المؤرخة في 16 نوفمبر 2008.

2) القانون 03-2000 المؤرخ في 05 أوت 2000 المحدد للقواعد المتعلقة بالبريد و المواصلات السلكية و اللاسلكية، المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية رقم : 48 الصادرة بتاريخ : 06 أوت 2000.

3) القانون 01-08 المؤرخ في 26 جوان 2001 المعدل و المتمم لأحكام قانون الإجراءات الجزائية الجزائري و المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية العدد رقم : 34 الصادرة يوم 27 جوان 2001.

4) القانون رقم 04-05 المؤرخ في 10 نوفمبر 2004 والمتضمن تعديل قانون العقوبات، المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية العدد رقم: 71 الصادرة يوم 10 نوفمبر 2004.

5) القانون 06-22 المؤرخ في 20 ديسمبر 2006 المعدل و المتمم لأحكام قانون الإجراءات الجزائية الجزائري و المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية العدد رقم : 84 الصادرة يوم 24 ديسمبر 2006.

6) القانون 08-01 المؤرخ في 23 جانفي 2008 المعدل و المتمم للقانون رقم 11/83 المتعلق بالتأمينات الاجتماعية، المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية رقم : 04 الصادرة بتاريخ : 27 جانفي 2008.

7) القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها، المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية رقم : 47 الصادرة بتاريخ : 16 أوت 2009.

III. الأوامر:

1) الأمر رقم 66 – 155 المؤرخ في 18 صفر عام 1386 الموافق 08 جوان سنة 1966، المتضمن قانون الإجراءات الجزائية الجزائري، المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية العدد رقم : 48 الصادرة يوم 10 جوان 1966.

2) الأمر رقم 66 – 156 المؤرخ في 18 صفر عام 1386 الموافق 08 جوان سنة 1966، المتضمن قانون العقوبات الجزائري، المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية العدد رقم : 49 الصادرة يوم 11 جوان 1966.

3) الأمر رقم 15–02 المؤرخ في 23 جويلية 2015 و المتضمن تعديل أحكام قانون الإجراءات الجزائية الجزائري ، المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية رقم : 40 الصادرة بتاريخ 23 جويلية 2015 .

IV. المراسيم:

1) المرسوم الرئاسي رقم 15–261 المؤرخ في 08 أكتوبر 2015 و المتضمن تحديد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها ، المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية رقم : 53 الصادرة بتاريخ : 08 أكتوبر 2015.

❖ ثانيا: المراجع المتخصصة.

1) خالد عياد الحلبي – إجراءات التحري و التحقيق في جرائم الحاسوب و الأنترنت– الطبعة الأولى – دار الثقافة للنشر و التوزيع – عمان– الأردن– 2011.

2) عبد الفتاح بيومي حجازي– الجوانب الإجرائية لأعمال البحث والتحقيق الإبتدائي في الجرائم المعلوماتية– دراسة مقارنة على ضوء القواعد العامة للإجراءات الجنائية– الطبعة الأولى– دار النهضة العربية– مصر– 2009.

3) علي حسن أحمد الطوالبة – التفتيش الجنائي على نظم الحاسوب و الانترنت– دراسة مقارنة– عالم الكتب الحديث – اربط– الأردن – 2004.

4) علي عدنان الفيل – إجراءات التحري و جمع الأدلة و التحقيق الإبتدائي في الجريمة المعلوماتية– دراسة مقارنة– دار الكتاب الجامعي الحديث– الإسكندرية– مصر– 2012.

5) محمد الأمين البشيري– التحقيق في الجرائم المستحدثة– مركز الدراسات و البحوث – جامعة نايف للعلوم الأمنية– الرياض– السعودية– 2004.

6) ممدوح عبد الحميد عبد المطلب– البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت– دار الكتب القانونية– مصر– 2007.

7) نبيلة هبة هروال– الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الإستدلالات – دار الفكر الجامعي– الإسكندرية– مصر – 2007.

❖ ثالثا : المراجع العامة.

1) أسامة أحمد المناعسة – جلال محمد القاضي – جرائم تقنية نظم المعلومات الإلكترونية–دراسة مقارنة– الطبعة الأولى– دار الثقافة للنشر و التوزيع – عمان –الأردن– 2010

2) العربي جنان – معالجة المعطيات ذات الطابع الشخصي – الحماية القانونية في التشريع المغربي و المقارن – الكتاب 2 – المملكة المغربية – 2010.

3) بولين أنطونيوس أيوب – الحماية القانونية للحياة الشخصية في مجال المعلوماتية – دراسة مقارنة – الطبعة الأولى– منشورات الحلبي الحقوقية– بيروت – لبنان– 2009.

4) حسن طاهر داود – جرائم نظم المعلومات – الطبعة الأولى– جامعة نايف للعلوم الأمنية – الرياض– السعودية – 2000.

5) سامي على حامد عياد– الجريمة المعلوماتية و إجرام الأنترنت– دار الفكر الجامعي – الإسكندرية – مصر – 2007.

6) ضياء علي أحمد النعمان– الغش المعلوماتي الظاهرة والتطبيقات– الطبعة الأولى– المطبعة الوطنية– المملكة المغربية– 2011.

7) عائشة بن قارة– حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري و القانون المقارن– دار الجامعة الجديدة – الإسكندرية – مصر – 2010.

8) عبد العال الدريبي – الجرائم الإلكترونية – دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية و الأنترنت – المركز القومي للإصدارات القانونية – القاهرة – مصر – 2012.

9) عبد الفتاح بيومي حجازي– الدليل الجنائي في جرائم الكمبيوتر و التزوير– دراسة معمقة في جرائم الحاسب الآلي و الأنترنت– دار الكتب القانونية– مصر– 2004.

10) عبد الفتاح عبد اللطيف الجبارة – إجراءات المعاينة الفنية لمسرح الجريمة–الطبعة الأولى– دار الحامد للنشر و التوزيع– عمان– الأردن – 2010–

11) عبد الكريم عبد الله عبد الله – الحماية القانونية للملكية الفكرية على شبكة الأنترنت – دار الجامعة الجديدة – مصر– سنة 2008.

12) علي بن عبد الله غسيري – الأثار الأمنية لأستخدام الشباب للأنترنت – الطبعة الأولى– جامعة نايف للعلوم الأمنية– الرياض – السعودية – 2004.

13) فتوح الشادلي – عفيفي كامل عفيفي – جرائم الكمبيوتر وحقوق المؤلف و المصنفات الفنية ودور الشرطة– منشورات الحلبي الحقوقية– بيروت – لبنان– دون ذكر سنة النشر.

14) محمد أمين الشوابكة – جرائم الحاسوب و الأنترنت(الجريمة المعلوماتية)– دار الثقافة للنشر و التوزيع– عمان–الأردن– 2009 .

15) محمد حسين منصور – المسؤولية الإلكترونية – دار الجامعة الجديدة – مصر –2003.

16) محمد حماد الهيتي– التكنولوجيا الحديثة و القانون الجنائي– الطبعة الثانية– دار الثقافة للنشر و التوزيع– عمان– الأردن– 2012.

17) محمد علي العريان – الجرائم المعلوماتية – دار الجامعة الجديدة – الإسكندرية– مصر – 2004.

18) محمد محمد محمد عنب– إستخدام التكنولوجيا الحديثة في الإثبات الجنائي– دون ذكر دار النشر– مصر – 2007.

19) محمود أحمد عبابنة– جرائم الحاسوب وأبعادها الدولية– دار الثقافة للنشر و التوزيع– الأردن– 2005.

20) ناير نبيل عمر – الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية – دار الجامعة الجديدة– مصر– سنة 2012.

21) نهلا عبد القادر المومني – الجرائم المعلوماتية – الطبعة الثانية– دار الثقافة للنشر و التوزيع– عمان– الأردن – 2010.

22) هلالي عبد اللاه أحمد – إتفاقية بودابست لمكافحة الجرائم المعلوماتية معلقا عليها – الطبعة الأولى– دار النهضة العربية – مصر – 2008.

23) يوسف حسن يوسف – الجرائم الدولية للانترنت – الطبعة الأولى– المركز القومي للإصدارات القانونية – القاهرة– مصر– 2011.

❖ **رابعا : الرسائل العلمية .**

1) إبراهيم بن سطم بن خلف العنزي – التوقيع الإلكتروني و حمايته الجنائية – رسالة مقدمة لأجل نيل شهادة الدكتوراه– قسم العلوم الشرطية – جامعة نايف للعلوم الأمنية – الرياض – السعودية– 2009.

2) تركي بن عبد الرحمان المويشير– بناء نموذج أمني لمكافحة الجرائم المعلوماتية و قياس فعاليته– رسالة مقدمة لأجل نيل شهادة الدكتوراه– قسم العلوم الشرطية – جامعة نايف للعلوم الأمنية – الرياض – السعودية – 2009.

3) عبد الله بن سعود محمد السراني – فعالية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني– رسالة مقدمة لأجل نيل شهادة الدكتوراه– قسم العلوم الشرطية – جامعة نايف للعلوم الأمنية – الرياض – السعودية – سنة 2009.

4) عمر بن محمد العتبي – الأمن المعلوماتي و مدى توافقه مع المعايير المحلية و الدولية – رسالة مقدمة لأجل نيل شهادة الدكتوراه – قسم العلوم الشرطية– جامعة نايف للعلوم الأمنية – الرياض – السعودية– 2010.

❖ **خامسا: المقالات العلمية .**

1) الهاشمي الكسراوي- "الجريمة المعلوماتية"- مقالة منشورة بمجلة القضاء و التشريع- العدد 07 – السنة 48- جويلية 2006- مركز الدراسات القانونية و القضائية- وزارة العدل و حقوق الإنسان- الجمهورية التونسية.

2) محمد أزيلاجي- "حجية دليل الحاسوب الآلي في النطاق الجنائي"- مقالة منشورة بالمجلة المغربية للمنازعات القانونية- عدد مزدوج 10-11- سنة 2010- دون ذكر هيئة النشر-وجدة- المملكة المغربية.

3) نزيهة مكاري-" وسائل الإثبات في جرائم الاعتداء على حق المؤلف عبر الانترنت"- مقالة منشورة بمجلة المناهج القانونية- العدد المزدوج 13-14 – سنة 2009- دون ذكر المعلومات المتعلقة بهيئة النشر- المملكة المغربية.

4) يوسف مسعودي –" النظام القانوني لحماية المصنفات الرقمية " – مقالة منشورة بمجلة الدراسات القانونية – العدد 04 – أوت 2009. مركز البصيرة للبحوث و الاستشارات و الخدمات التعليمية – الجزائر .

❖ **سادسا: المؤتمرات و البحوث.**

1) رضا هميسي- أحكام الشاهد في الجريمة المعلوماتية- بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة- 16و 17 نوفمبر 2015- كلية الحقوق – جامعة بسكرة- الجزائر.

2) سامية بلجراف- سلطة القاضي الجنائي في قبول و تقدير الدليل الرقمي- بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة- 16و 17 نوفمبر 2015- كلية الحقوق – جامعة بسكرة- الجزائر.

3) سلمى مانع – دور الأمن المعلوماتي في مكافحة الجرائم المعلوماتية- بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة- 16و 17 نوفمبر 2015- كلية الحقوق – جامعة بسكرة- الجزائر.

4) عبد الرحمان حملاوي- دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية- بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة- 16و 17 نوفمبر 2015- كلية الحقوق – جامعة بسكرة- الجزائر.

5) عبد الله حسين علي محمود- "إجراءات جمع الأدلة في مجال سرقة المعلومات"- بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الإلكترونية – مركز البحوث و الدراسات- أكاديمية شرطة دبي- دبي- الإمارات العربية المتحدة- من 26 إلى 28 أفريل 2003.

6) عبد المؤمن بن صغير- الطبيعة الخاصة للجريمة المرتكبة عبر الأنترنت في التشريع الجزائري و المقارن- بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة- 16و 17 نوفمبر 2015- كلية الحقوق – جامعة بسكرة- الجزائر.

7) عزالدين عزالدين – قيادة الدرك الوطني- الإطار القانوني للوقاية من الجرائم المعلوماتية و مكافحتها – بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة- 16و 17 نوفمبر 2015- كلية الحقوق – جامعة بسكرة- الجزائر.

8) علي محمود حمودة-" الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي"- مقالة مقدمة للمؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الإلكترونية – من 26 إلى 28 أفريل 2003- مركز البحوث و الدراسات- أكاديمية شرطة دبي- دبي- الإمارات العربية المتحدة.

9) موسى مسعود أرحومة- الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية- بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية و القانون - 28 - 29 أكتوبر 2009- أكاديمية الدراسات العليا- طرابلس - ليبيا.

❖ **سابعا : زيارات ميدانية.**

1) ملخص الزيارة الميدانية لدائرة الأدلة الرقمية و الآثار التكنولوجية - المخبر الجهوي للشرطة العلمية لولاية قسنطينة بتاريخ : 01 أفريل 2015.

❖ المصادر الإلكترونية.

❖ **أولا : الكتـــب.**

1) محمد سيد سلطان - قضايا قانونية في امن المعلومات و حماية البيئة الإلكترونية- دار ناشري للنشر الإلكتروني - الكويت- سنة 2012. مرجع متوفر على الموقع الرسمي لدار ناشري للنشر الإلكتروني- تاريخ التصفح: 2015/02/05 -الرابط الإلكتروني:

http://www.nashiri.net/latest/books-mags-news/5051-2012-01-27-22-05-28-v155-051.html

❖ **ثانيا : المقالات العلمية .**

1) حسين فريجه- "الجرائم الإلكترونية و الأنترنت" - مقالة علمية منشورة بمجلة المعلوماتية - العدد 36- أكتوبر 2011-وكالة التطوير و التخطيط- وزارة التربية و التعليم - السعودية - متوفرة على شبكة الأنترنت - تاريخ التصفح : 2013/06/26 الرابط الإلكتروني :

www.informatics.gov.sa/articles.php?artid=586

❖ **ثالثا: البحوث و الدراسات.**

1) حسين بن سعيد الغافري-" التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الأنترنت"- بحث منشور على الموقع الإلكتروني الرسمي للمركز العربي للبحوث القانونية و القضائية للجامعة العربية- تاريخ التصفح: 03/23/ 2012- الرابط الإلكتروني:

http://www.carjj.org/node/1376

2) علي حسن أحمد الطوالبة-"إجراءات ضبط المكونات المعنوية للحاسوب و الانترنت"- بحث منشور على الموقع الإلكتروني لمركز الإعلام الأمني- أكاديمية الشرطة البحرينية- مملكة البحرين- أفريل 2011- تاريخ التصفح 2014/05/29 الرابط الإلكتروني:

http://www.policemc.gov.bh/reports/2011/April/30-4-2011/634397721383881294.pdf

3) علي حسن أحمد الطوالبة- "مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي" - بحث منشور على الموقع الإلكتروني لمركز الإعلام الأمني- أكاديمية الشرطة البحرينية- مملكة البحرين- أفريل 2011- تاريخ التصفح 2014/05/29 الرابط الإلكتروني:

www.policemc.gov.bh/reports/2011/April/13-2011/634383168746341670.pdf

4) محمد علي قطب -" الجرائم المعلوماتية وطرق مواجهتها" - الجزء الأول- بحث منشور على الموقع الإلكتروني لمركز الإعلام الأمني- أكاديمية الشرطة البحرينية- مملكة البحرين- أفريل 2011- تاريخ التصفح: 2014/06/05 الرابط الإلكتروني:

www.policemc.gov.bh/reports/2011/April/1-4-2011/634372714052375622.pdf

5) محمد علي قطب – الجريمة المعلوماتية و طرق مواجهتها – الجزء الثالث – بحث منشور على الموقع الإلكتروني لمركز الإعلام الأمني– أكاديمية الشرطة البحرينية– مملكة البحرين– أفريل 2011– تاريخ التصفح: 2014/06/05 الرابط الإلكتروني:

www.policemc.gov.bh/reports/2011/April/12-4-2011/634382244195974306.pdf

6) "منظومة I-Link الربط بين التحقيقات في العالم أجمع"– بحث متوفر على الموقع الرسمي للأنتربول – النسخة العربية– تاريخ التصفح: 2014/08/08 الرابط الإلكتروني:

www.interpol.int/content/download/789/342185/version/21/file/05_GI05_08_2013_AR_web.pdf

7) "لمحة عن الأنتربول"– بحث متوفر على الموقع الرسمي للأنتربول الدولي– النسخة العربية–تاريخ التصفح: 25-05 -2014 – الرابط الإلكتروني :

http://www.interpol.int/content/download/785/342162/version/22/file/01_GI01_03_2014_AR_web.pdf

❖ رابعا :التقارير السنوية و الإحصائية.

1) التقرير السنوي لنشاط الأنتربول لسنة 2012– متوفر على الموقع الرسمي للأنتربول–النسخة العربية– تاريخ التصفح: 2014/04/12 الرابط الإلكتروني:

www.interpol.int/content/download/20552/185417/version/5/file/Annual%20Report%202012_AR_i.pdf

2) تقرير مجموعة العمل الحكومية المشتركة الفرنسية تحت عنوان – حماية مستعملي شبكة الأنترنت– فيفري 2014– متوفر على الموقع الرسمي لوزارة العدل الفرنسية – تاريخ التصفح: 2015/03/05 الرابط الإلكتروني: http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf

3) التقرير الإحصائي السنوي للواقع الرقمي حول العالم لسنة 2014 – "The Global Digital Statistic 2014" – متوفر على شبكة الأنترنت – تاريخ التصفح: 2015/01/05 – الرابط الإلكتروني:

http://etonpreneurs.com/uploads/Global%20Social,%20Digital%20&%20Mobile%20Statistics,%20Jan%202014.pdf

❖ **خامسا : مواقع إلكترونية .**

1) الموقع الرسمي لقيادة الدرك الوطني – تاريخ التصفح 31 مارس 2015 – الرابط الإلكتروني :

http://www.mdn.dz

2) الموقع الرسمي للمديرية العامة للأمن الوطني– تاريخ التصفح 23 فيفري 2015– الرابط الإلكتروني:

www.dgsn.dz

3) موقع الإحصائيات العالمية –تاريخ التصفح 2014/05/05– الرابط الإلكتروني:

www.internetworldstats.com

4) موقع جريدة :Le Figaro على الرابط الإلكتروني التالي :

www.lefigaro.fr

❖ **المراجع باللغة الأجنبية .**

I- Les ouvrages en français.

1) Céline Renard Castétes – Cours de Droit de l'internet – Edition 2010 – Edition Lex tenso – Paris – France- 2010.

2) Charle Diaz – La Police Techenique et Scientifique–2eme Edition– Edition Presse universitaire de France – France – 2006.

3) Eric Filiol et Philippe Richard– Cyber Criminalité–enquête sur les mafias qui envahissent le web– Edition Dunod–paris –France– 2006.

4) –Jean Claude martin – investigation de scènes de crimes –fixation de l'état des lieux et traitement des traces d'objet– presse polytechnique et universitaire Romandes– France– 2004.

5) Jean Michel Bruguière – Le Droit de l'internet – lois contrat et usage – Edition Litec– Paris – France – 2009.

6) Mohamed Chawki – Combattre la cybercriminalité – Edition de saint Amans– Paris – France– Mai 2009.

7) Myriam Quéméner – Joël Ferry– Cybercriminalité Défi mondial– Edition Economica – Paris – France–2009.

8) Myriam Quéméner– Jean Paul Pinte – Cybersécurité– Edition Hermès science– Lavoisier– Paris– France 2013.

9) Myriam Quéméner– Yves Charpenel – La Cybercriminalité– Edition Economica– Paris– France–2010.

II–Les thèses .

1) Feverier Rémy–Management de la sécurité des systèmes d'information : Les collectivités territoriales face au risque numérique– Thèse de Doctorat– Ecole Doctoral de science Economique et de gestion– université Paris 02– France – Avril 2012.

2) Jean– Philippe Humbert– le mondes de la cyber délinquance et l'image sociale du pirate informatique – thèse de doctorat– sciences de l'information est de la télécommunication – université Paul Verlaine –Metz – France – 2007.

III–Les articles.

1) Adeline Champagnat–« L'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication » Article publié sur la revue : cybercriminalité cybermenace et cyberfraude – sous la direction de : Irène Bouhadana et William Gilles – Edition– IMODEV– Paris– France–2012.

2) Charlie Abrahams –« La Cybercriminalité un Business Croissant lié à l'éffondrement des crédits »– Article publier dans la revus de la sécurité Globale– numéro 06– année 2008– Disponible sur site : www.carin.info – Fond documentaire (S.N.D.L) Système national de documentation en ligne – Algérie– Date de consultation 28 /03/2014.

3) Eugéne Kaspersky – "Défis de la cybercriminalité" – Article publié dans la revus de la sécurité Globale– numéro 06 – année 2008– Disponible sur site : www.carin.Info– Fond documentaire (S.N.D.L) Système national de documentation en ligne – Algérie– Date de consultation 28 /03/2014.

4) Gérard SCHOEN –« La douane face a la cybercriminalité »– Article publié sur la revue : cybercriminalité cybermenace et cyberfraude – sous la direction de : Irène Bouhadana et William Gilles – Edition– IMODEV– Paris– France–2012.

5) Joël Rivière et Didier Lucas –« Criminalité et internet une arnaque à bon Marché » – Article publier dans la revus de la sécurité Globale– numéro 06– année 2008– Disponible sur site : www.cairn.info – Fond documentaire (S.N.D.L) Système national de documentation en ligne – Algérie– Date de consultation 28 /03/2014.

6) Myriam Quémnéner –« La Coopération Entre les Organes de Lutte Contre la Cybercriminalité – pour une stratégie globale de cybersécurité Français » – Article publier sur La Revue Electronique : Lamy Droits des affaires –Num 87– France – 2013.

7) Sofia Belghiti – "Les mineurs et les infractions a l'internet "– Article publier sur la Revue marocaine de l'enfant et de la famille – Num 01–janvier 2010 – le royaume Marocain.

8) William Gilles et Jean Harivel et Iréne Bouhadana –« Darknet le coté obscur du net »– Article publier sur : Panthéon Sorbonne Magazine – Magazine D'information de L'université Paris 1 Panthéon Sorbonne – Num 06– Janvier – Février – 2014– Paris – France.

IV– Les Exposés.

1)–Frédérique Chopin– La Cybercriminalité– Exposé publié sur L'Encyclopédie Electronique : Le Répertoire de Droit pénal et de Procédure Pénale – paris–France–juillet– 2013.

V– Les Rapports .

1)– François sopin – Rapport sur l'actualité de cybercriminalité en 2012 – Article disponible sur internet – Date de consultation 03/06/2014- lien directe : https://www.adacis.net/wpcontent/uploads/2012/12/ADACIS_CLUSIRA_Cyber criminalit%C3%A9_2012.pdf

2)– La situation de la Convention sur la Cybercriminalité–Traité de Budapest – Disponible sur le site officiel du Conseil de l'Europe –Date de consultation 03/06/2014- lien direct : http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=20/07/2014&CL=FRE

الفهرس

الفصل الأول: الإطار المفاهيمي للجريمة المعلوماتية.

الفصل الثاني :مسألة شرعية إجراءات البحث و التحقيق في الجرائم المعلوماتية و الجهات المختصة بتنفيذها .

الفصل الثالث: الإجراءات الخاصة بالبحث و التحقيق في الجرائم المعلوماتية و آثارها.

الملخصات باللغتين–العربية و الفرنسية

ملخص :

لقد عرفت حياة الإنسان في هذه السنوات الاخيرة تطورا لم يسبق له مثيل ، و ذلك بفعل التطور المذهل لتقنية المعلوماتية و إنتشارها اللامحدود ، كما تنامت إلى جانب ذلك التهديدات أكثر بفعل إنتشار نوع جديد من الجرائم يضاف إلى قائمة الجرائم التي كانت معروفة مسبقا و هي الجرائم المعلوماتية، التي أصبحت تشكل أكبر و أخطر تهديد على أمن الدول و المجتمعات ، و هو ما جعل من موضوعها من اهم المواضيع المطروحة في ميدان البحث العلمي القانوني، و ذلك بفعل الإشكاليات العديدة التي تطرحها هذه الجرائم و بالخصوص الإجرائية منها و المتعلقة بآليات البحث و التحقيق الجنائي في مجال مكافحة الجرائم المعلوماتية ، و هو ما دفع بنا إلى إختيار هذا الموضوع بهدف إختبار مدى فعالية الإجراءات الجزائية في ظل مختلف النصوص القانونية المستحدثة و الخاصة بالبحث و التحقيق في الجرائم المعلوماتية ، في مواجهة الطبيعة الخاصة و التعقيدات التقنية التي تمييز هذه الجرائم .

لقد تضمنت الدراسة في هذا المجال معطيات قانونية و أخرى فنية و تقنية نظرا لطبيعة الموضوع الذي يعتبر نقطة تقاطع بين علوم الحاسوب و النظم المعلوماتية و العلوم القانونية الإجرائية ، و لذلك فقد عالجنا في إطار ثلاث فصول مختلف الجوانب المتصلة بالموضوع من أجل الوصول إلى مفاهيم قانونية حديثة تتماشى و طبيعة الجرائم المعلوماتية ، فعالجنا في إطار الفصل الأول مفهوم تقنية المعلوماتية بإعتبارها الوعاء المنطقي للجريمة المعلوماتية و الإجراءات الخاصة بالبحث و التحقيق بشأنها ، كما تناولنا بالتعريف الجريمة المعلوماتية ذاتها من كافة النواحي الفقهية منها و الإصطلاحية و القانونية ، خصوصا و ان هذا المجال يعتبر من أكثرها تفاعلا و ديناMكية بفعل إستحداث و تحديث مختلف المفاهيم المتعلقة بالجريمة المعلوماتية بالنظر إلى التطور الدائم الذي يميز الجرائم المعلوماتية ، و قد إرتكزت دراستنا على تحليل و مقارنة مختلف الآراء الفقهية و النصوص القانونية على شاكلة قانون العقوبات

الجزائري و القانون 09-04 المتعلقة بالوقاية و مكافحة الجرائم المعلوماتية ، بالإضافة إلى مختلف النصوص القانونية المقارنة من نفس النوع ، و هو ما سمح لنا بتحديد دقيق لمفهوم و صور الجرائم المعلوماتية ، بالإضافة إلى توضيح مدى تعقيدها من حيث أساليب تنفيذها و أثارها.

اما موضوع دراستنا في إطار الفصل الثاني فقد تمحور حول دراسة مدى إنقسام الفقه و القانون حول مدى إعتبار الفضاء الرقمي و الجرائم المعلوماتية محلا لإجراءات البحث و التحقيق الجنائي ، و مدى تأقلم القانون مع هذا التوجه المستحدث للنصوص الإجرائية ، خصوصا و ان الجريمة المعلوماتية قلبت كل المفاهيم التقليدية التي كانت تحكم الجرائم التقليدية و على رأسها الطابع المادي للجرائم و مبدأ إقليمية النص الجنائي ، من خلال استعراض مختلف الجهود القانونية المبذولة على مختلف الأصعدة الدولية منها و الوطنية في سبيل دعم آليات البحث و التحقيق في الجرائم المعلوماتية ، و تذليل العقبات التي تفرضها الطبيعة الخاصة لهذه الجرائم ، بالإضافة إلى إستعراض مختلف الهيئات الخاصة المكلفة بإجراءات البحث و التحقيق بشأن الجرائم المعلوماتية بما فيها الدولية و الإقليمية و الوطنية الداخلية ، و قد ركزنا دراستنا في هذا المجال حول الهيئات المكلفة بالبحث و التحقيق المنتمية إلى مختلف الهيئات سواء الأمنية كمصالح الشرطة و الدرك أو الخاصة، و ذلك في التشريع الفرنسي و بالخصوص في التشريع الجزائري خصوصا في ظل المتغيرات الأخيرة و التي شهدت تنصيب الهيئة الوطنية المكلفة بالوقاية و مكافحة الجرائم المعلوماتية بتاريخ الـ8 أكتوبر 2015.

اما في الفصل الثالث و الأخير من بحثنا هذا فقد حاولنا ان نلم بالدراسة بكل الجوانب الفنية و القانونية التي تحكم عمل المحققين في مجال الجرائم المعلوماتية ، من خلال إبراز جملة الخصائص المعرفية التقنية و القانونية التي يجب ان تميز المحقق في مجال البحث و التحقيق في الجرائم المعلوماتية ، بالإضافة إلى التعرض إلى مختلف الإجراءات السابقة و المعاصرة و اللاحقة لمختلف الإجراءات

المتخذة في مجال البحث و التحقيق في الجرائم المعلوماتية ، لنختتم فصلنا هذا بالتعرض إلى آثار أعمال البحث و التحقيق في الجرائم المعلوماتية و مدى حجيتها في الإثبات بالنظر إلى طبيعتها الإلكترونية الخاصة ، و إلى جملة معوقات البحث و التحقيق في مجال الجرائم المعلوماتية و التي لا زالت تشكل بذاتها التحدي الأكبر في مجال ضمان فعالية قصوى للإجراءات المتخذة في سبيل مكافحة الجرائم المعلوماتية.

لتختتم بحثنا بخاتمة حاولنا من خلالها الخروج بأكبر قدر ممكن من النتائج التي تفيد في الإجابة عن الإشكالية الأساسية و الإشكاليات الفرعية، مع تحصيل مجموعة من التوصيات القانونية التي من شانها دعم آليات البحث و التحقيق في الجرائم المعلوماتية.

Résumé : Le développement des nouvelles technologies de l'information ouvre un nouvel espace comme L'espace Numérique qui vient s'ajouter aux espaces terrestre, maritime et aérien, dont la protection et la sécurité entrent naturellement dans le champ des compétences de l'Etat. Espace virtuel, par sa structure et la nature même des informations qu'il véhicule, le cyberespace a des incidences concrètes sur la vie quotidienne, notamment en ce qui concerne l'accès à la connaissance, les communications entre les personnes, le commerce, l'administration...etc.

Toute activité, toute invention humaine porteuse de progrès, peut être aussi génératrice de comportements illicites. La cybercriminalité est l'une des nouvelles formes de criminalité, dont les conséquences peuvent être particulièrement graves pour notre sécurité collective, et bien sûr pour les citoyens qui peuvent être personnellement atteints, dans leur personne, dans leur dignité et dans leur patrimoine. Le caractère virtuel des échanges qui débutent sur Internet favorise le franchissement des barrières de l'illégalité, les internautes ayant le sentiment que les bornes morales ou légales de la vie réelle ne s'appliquent pas au cyberespace, ce dernier leur paraissant totalement "désincarné".

La cybercriminalité est un nouveau thème de recherche pour le droit pénal et la procédure pénale, c'est pour cela que nous l'avons choisi comme sujet d'étude, vus les nombreuse problématiques que pose ce sujet surtout en matière d'application de loi pénal et la procédure pénale.

Notre étude a été devisé en trois grands chapitres, chacun consacré pour traité un champ spécifique de la cybercriminalité, le premier chapitre avait pour titre : La Définition de la cybercriminalité, on a procéder a définir en primer lieux la technologie de l'informatique et les systèmes informatiques considéré comme la scène principales des crimes informatiques, puis on est passé a la définition de la cybercriminalité avec objectif de bien préciser son concept juridique au milieu des nombreuse définitions proposer par la doctrine ,et la loi 09-04 promulgué en 2009 portant les règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication ,et les différentes lois comparées.

Le thème de notre étude dans le cadre du deuxième chapitre a porté sur l'étude du conflit entre les différents doctrine à propos de la mesure dans laquelle les crimes informatiques peuvent être soumis aux différentes

procédures de recherche et d'enquête criminelle, et l'étendue de l'a adaptation des dispositions de loi procédurales vis a vis ces nouvelles formes de criminalité , en plus on a essayer d'étudier les divers organismes charger de lutter contre la cybercriminalité , que se soit sur le niveau international comme l'interpole où, régional comme l'Europol ou bien national, et a ce niveau la on a focalisé notre étude sur les instances chargées d'enquêter sur les affaires liées a la cybercriminalité, affilies a la policière et a la gendarmerie , sur le plans de la législation française et en particulier dans la législation algérienne, surtout avec les changements récents ,vu l'installation de l'organisme national chargé de la prévention et de la lutte contre les crimes informatiques le 8 Octobre à 2015.

Alors que la troisième partie de cette recherche c'est concentré principalement sur l'étude des particularités des conditions techniques et juridiques qui doivent être observées par l'investigateur en matière de cybercriminalité , pour bien assuré la légitimité des procédures d'une part , et la fiabilité des procédures prise d'une autre part , vus que la nature de la cybercriminalité impose l'utilisation de nouvelles formes de procédures de recherche et d'investigation, souvent différentes de celle prise envers les crime traditionnels, la fin de ce troisième chapitre a été consacrer pour le sujet de la preuve numérique, et les nombreuse difficultés qui s'oppose devant les investigateurs dans le domaine de la cyber investigation, et qui empêchent souvent de découvrir les crime informatique, et l'arrestation des cybercriminels.

A la fin on a essayé de conclure nos efforts dans une conclusion qui résume un bon nombre de résultats et de perspectives ,qui peuvent résoudre les problèmes que pose la cybercriminalité dans de le domaine de cyber investigation.